Paul Pinault

Blog/contact : www.disk91.com
Twitter : @disk_91
YouTube: https://www.youtube.com/c/PaulPinault

The Internet Of Things

Introduction to what is the Internet of Things, why does it change the world where we live, what are the technologies behind the scene ?
How des it apply to your domain ?

- ISIMA ENGINEER
- 17 years MICHELIN IT, IoT
- CLOUD ARCHITECTE beys shared services

I'm building a secured cloud solution to host sensitive data like heath data, personal data, industrial secrets….

- IoT Expert

https://www.disk91.com
https://youtube.disk91.com
https://github.com/disk91/stm32-it-sdk

LoRaWAN sigfox

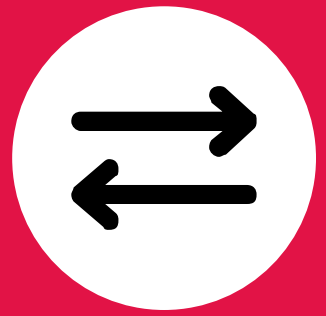
- DEVICE MAKER & STARTUP FOUNDER ingeniusthings
- TEACHER and SPEAKER

IoT is a solution, based on data collected from physical world, directly, by things

IoT has 3 layers to compose a solution.

DEVICES

To capture the data from the physical world
Devices are numerous. Larger the fleet is and larger the value created by the platform will be.



COMMUNICATION

To transmit, autonomously, the captured data from the fields to the consumers.
Communication key feature is not to be fast; it is to be energy efficient.

PLATFORM

Makes the data meaningful and accessible to the end-user.
Process large set of data. Mix different source of data. Create individual and aggregated value.
Manage the device fleet

FITBIT USE CASE

Get personal activity & health data from million of different people world-wide. Process them and propose:

- Individual feedback
- Global data studies and partnership programs

MULTIPLE DEVICES

Collecting the same type of Data

USING BLUETOOTH

And the customer smartphone as a Gateway to internet

WITH APP AND BIG DATA

To propose a valuable customer experience and B2B services like heath insurances

NETATMO USE CASE

Get home environmental information – Temperature, Hygro, Sound…

- Individual feedback
- Global data studies and partnership programs

MULTIPLE DEVICES

Collecting the different type of data all related to your home

USING Wi-Fi

And the customer Internet connectivity to reach the backend services

WITH APP AND BIG DATA

To propose a valuable customer experience and B2B services like city map of environmental noise

Let’s make a short break

LEARNING AT THIS STEP

IoT is a Solution

Composed by Hardware, Network and Software.
It needs maintenance and the associated business model is a service

Belonging on multiple technologies

The communication layer uses different technologies depends on the context.

With a two sides source of value

A direct benefit for the end-user (the reason why he buy it) and a B2B source of revenue obtained thanks to the massification of the collected data

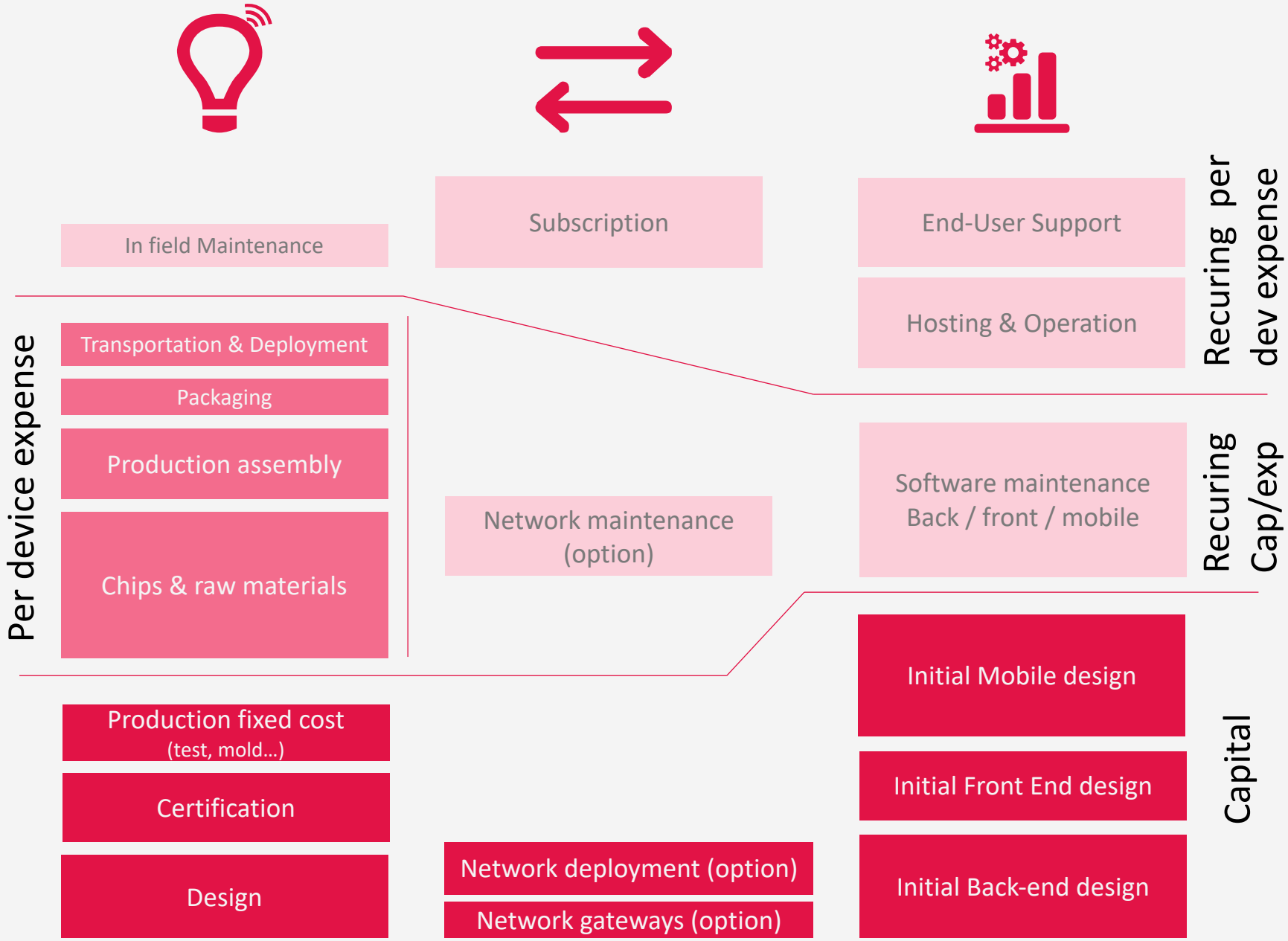
IoT solutions have a complex cost model

Mixing
- Capital to produce the software / hardware and industrialization design
- Per devices costs related to production and distribution
- Recuring investment to maintain the software stack
- Recuring cost for supporting maintenance, communications, platform run and end-user-support

1 **Volume of devices is a key factor**

2 **Longer the service is delivered and higher the cost per device is**

IoT solution business model differ from commodity product standard



HARDWARE ONLY

Xiaomi -Caméra de Sécurité Domestique 360° 1080P-Blanc

Visiter la boutique Xiaomi

4,4 ★★★★☆ 2 442 évaluations | 177 questions avec réponses

Prix conseillé : ~~39,99 €~~

Prix : 33,98 €

Économisez : 6,01 € (15 %)

Tous les prix incluent la TVA.

Assistance produit Amazon gratuite incluse

Livraison GRATUITE (0,01€ pour les livres) **en point retrait.** Détails

Neufs (9) à partir de 33,98 € + Livraison GRATUITE

IoT ORIENTED SOLUTION

Arlo Pro 3 | Pack de 2 caméras de surveillance 2K HDR, Batterie rechargeable Alarme Grand angle 160°, Audio Bi-directionnel Eclairage spotlight intégré (VMS4240P)

Visiter la boutique Arlo

4,1 ★★★★☆ 82 évaluations | 8 questions avec réponses

Prix : 599,00 €

Tous les prix incluent la TVA.

Payez: 149,75 € x 4 (~~13,48~~ 0 € de frais inclus) Voir conditions et plus de facilité de paiement

Assistance produit Amazon gratuite incluse

IoT needs recurring revenue or needs to includes future costs in the initial price

HARDWARE ONLY

Hangang Traceur GPS Magnétique 90 Jours Longue Veille IP65 étanche Suivi en Temps Réel, Tracker GPS pour Voiture Camion Moto Véhicule Outo TKMARS905

Marque : HanGang

★★★★☆ 125 évaluations | 104 questions avec réponses

Prix : 52,99 €

Tous les prix incluent la TVA.

Coupon Utiliser le coupon de 5% Détails

Payez en 4 fois dès 75 € d'achats Voir détails et conditions

Message promotionnel Promo... 3 promotions

Assistance produit Amazon gratuite incluse

Livraison GRATUITE (0.01€ pour les livres) en point

IoT ORIENTED SOLUTION

Passez la souris sur l'image pour zoomer

Tractive Collier Gps pour Chien - Traceur Gps avec Portée Illimitée, Blanc

Visiter la boutique Tractive

★★★★☆ 3 540 évaluations | 45 questions avec réponses

Prix conseillé : ~~49,00 €~~ De quoi s'agit-il?

Prix de l'offre : 19,19 €

Économisez : 29,81 € (61 %)

Tous les prix incluent la TVA.

Livraison GRATUITE (0.01€ pour les livres) **en point retrait.** Détails

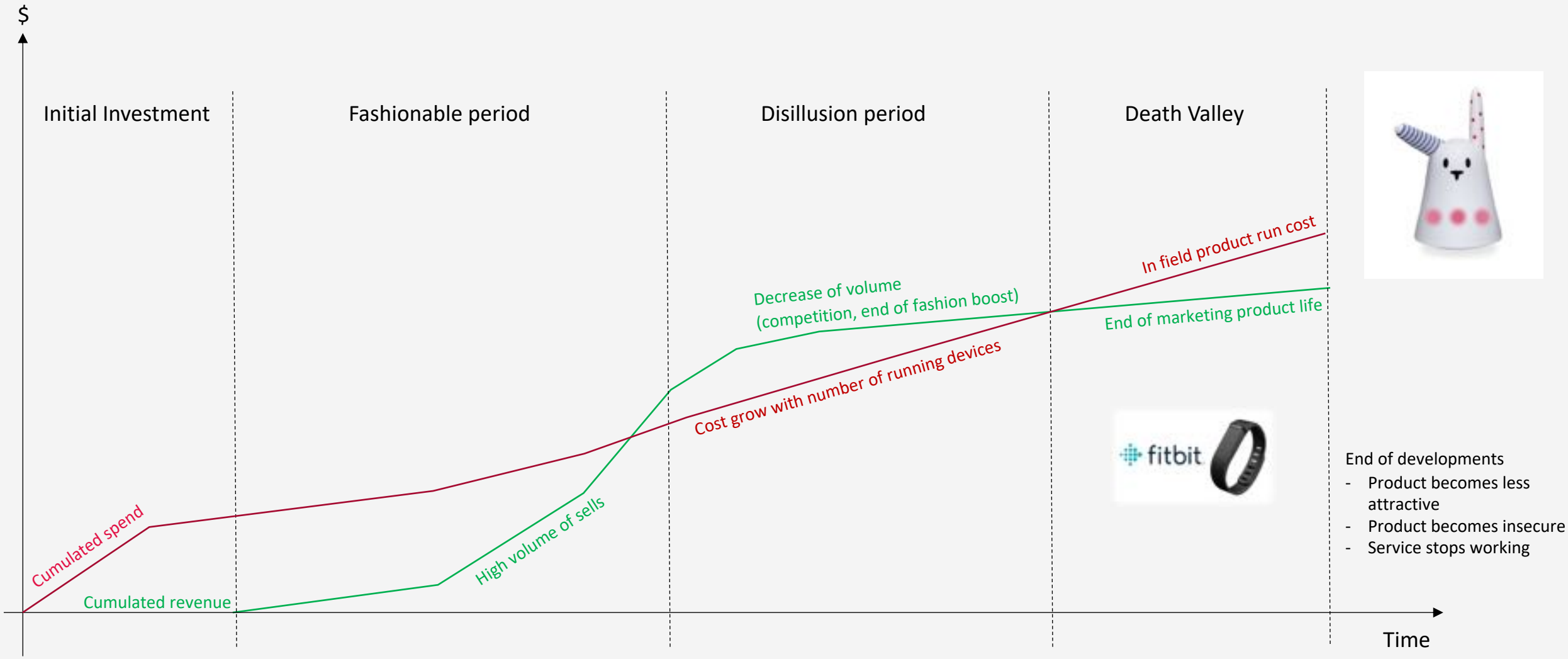
Neufs & occasions (7) 18,91 € et livraison GRATUITE pour les commandes d'un montant supérieur à 25,00 €

- ABONNEMENT REQUIS : à partir de 3,75 € par mois (pour abonnement biennal payable à l'avance), plusieurs options disponibles. L'appareil fonctionne grâce à une carte SIM déjà intégrée, et nécessite donc un abonnement Tractive couvrant la connexion mobile.
- TRACEUR GPS : Appareil de suivi GPS léger (35 g) et étanche, recommandé pour les chiens de plus de 4,5 kg. Le traceur Tractive GPS s'attache facilement à tout collier ou harnais. Contrairement aux GPS Bluetooth, le traceur Tractive a une portée illimitée.

Tractive GPS nécessite un abonnement afin de pouvoir suivre votre chien

Recurring revenue is a warranty for platform evolutions and data safety.

Selling IoT as a Product leads to slow death



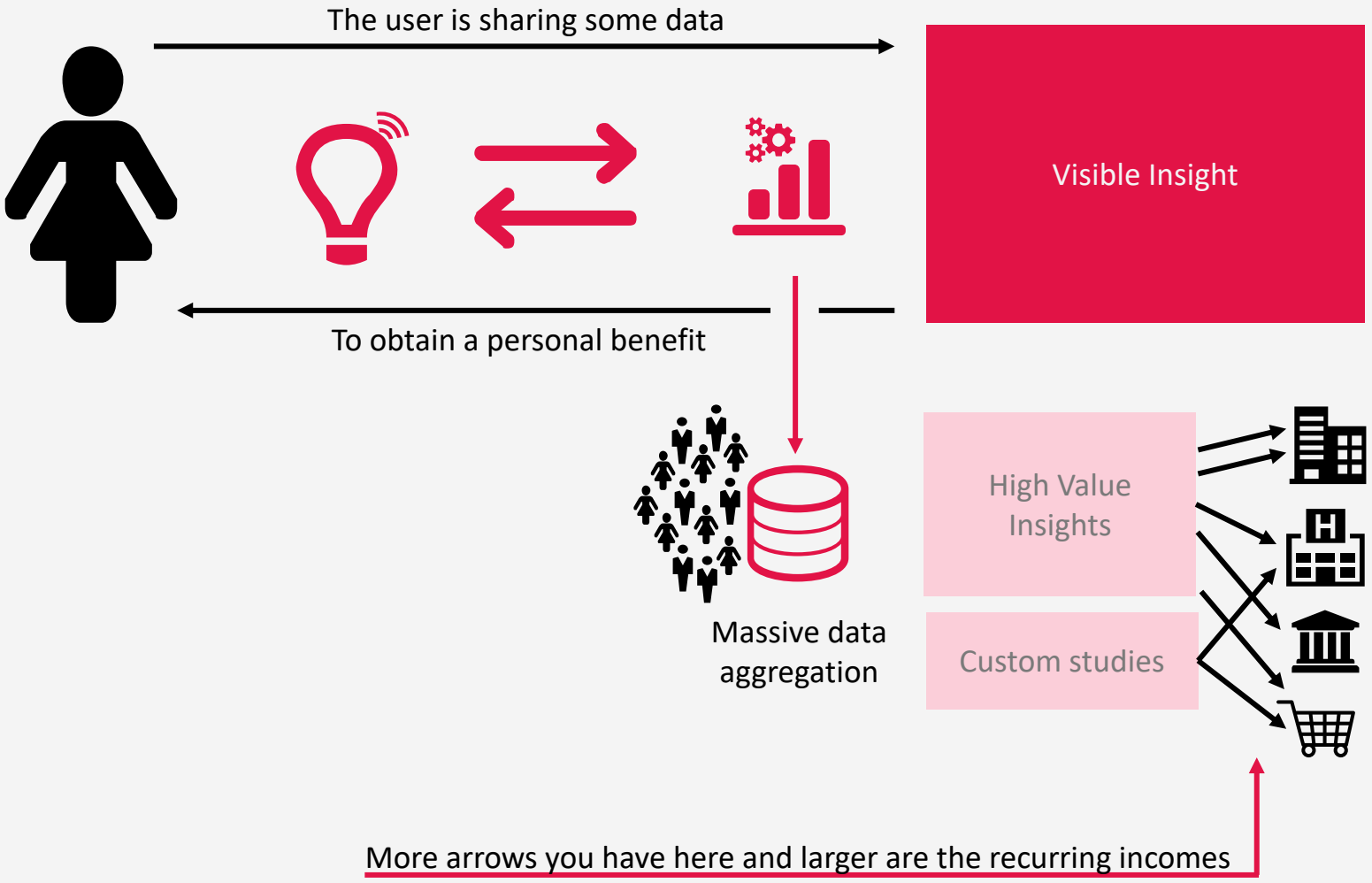
IoT revenue model

There are many revenue model, an illustration here is on B2C direct solution with indirect B2B markets

1 **There is the reason why you accept / want the solution.**

2 **There are the market where the solution creates value, sometime the reason why the solution has been created.**

This is a win-win deal for human generated data



“DATA IS THE NEW OIL” is a wrong assumption ! However data is ore.

MORE DATA YOU HAVE HIGHER ITS VALUE IS.

With larger data set you can extract more value, touch larger indirect businesses.

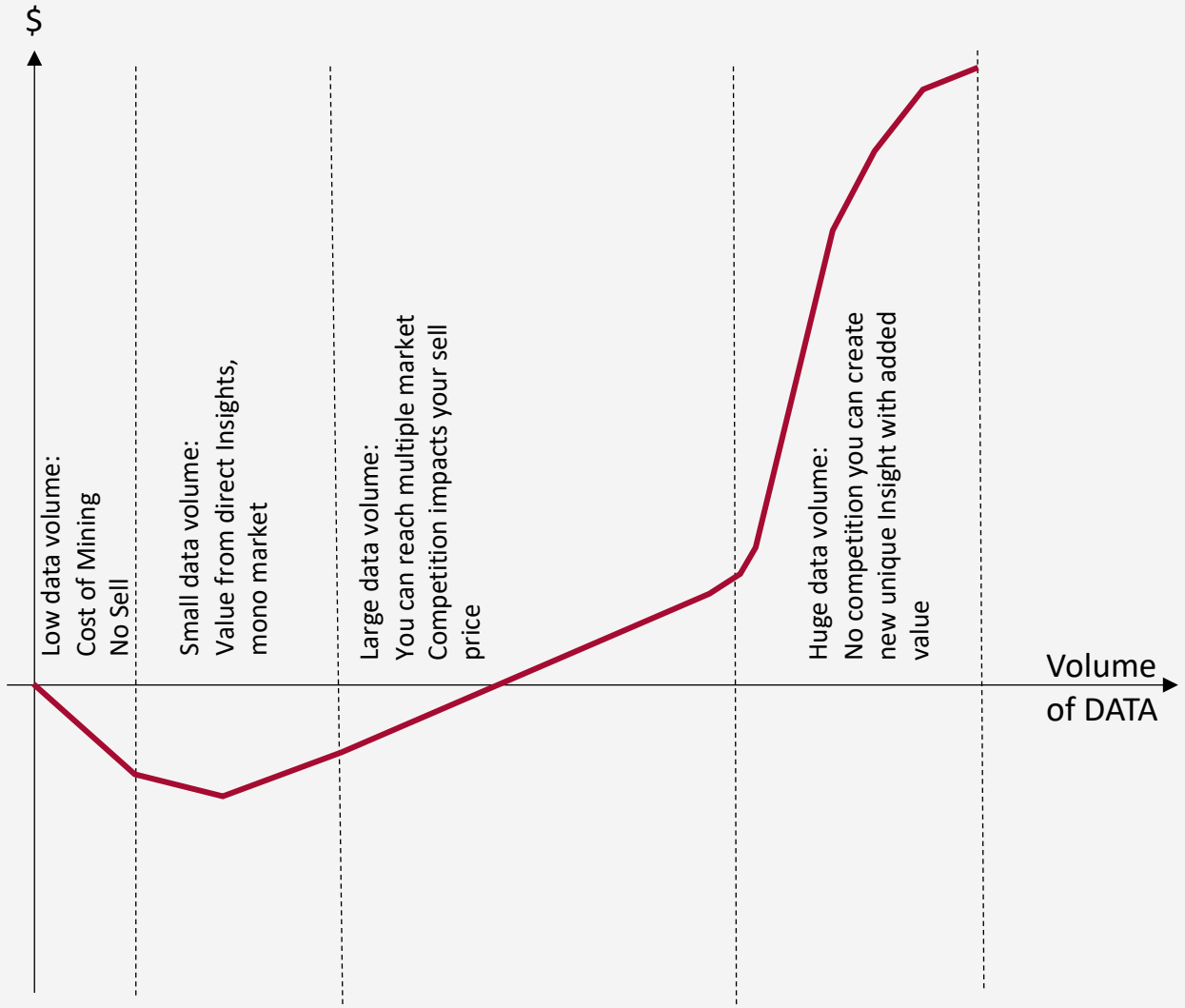
THE VALUE OF DATA IS ONLY DUE TO ITS UNIQUENESS

As the data can be sold without reducing your stock of Data, its value comes to a non existing competition or its value tends toward 0.

The rules of the DATA ORE

Mining data let you make a stock; the stock values comes from the number of markets/customers you can reach with unique Insights. This is related to the volume of data you have and the lack of competition. Selling you raw data is making new competitors.

- **DATA MINING HAS A COST**
- **DATA CAN BE REUSE INDEFINITELY**
- **SELLING RAW DATA DESTROY ITS VALUE**
- **DATA VALUE COMES FROM YOUR STOCK OR RAW DATA**
- **ANY COMPETITOR HAVING MORE DATA THAN YOU DESTROY YOUR DATA VALUE**



FITBIT USE CASE

Fitbit was the first to capture the human activity at a scale never obtained before. They have been able to propose unique Insights to health research, insurance market and much more. They were expecting a significant revenue from it to support the run costs.

I send information about my physical activity

I get report, challenges…

Visible Insight

Massive data aggregation

Global statistics (anonymous)

Profiling (personal data)

FITBIT USE CASE

The activity sensors have been deployed in cellphone, watches and many competitor's activity trackers making the activity data value tending toward zero today.

I send information about my physical activity

I get report, challenges…

Visible Insight

Massive data aggregation

Global statistics (anonymous)

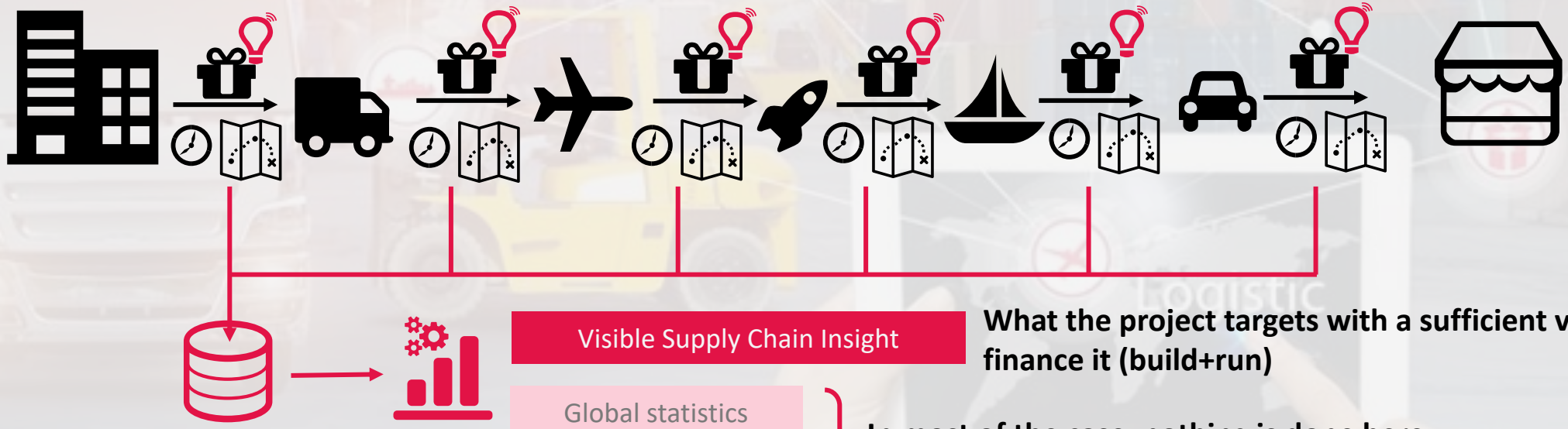
Profiling (personal data)

COMPETITORS

- Google
- Apple
- Samsung
- Strada
- Nike
- …

B2B Logistic Use-Case

With a tracker deployed in the element of the logistic chain, many companies are looking to improve the supply-chain cost by reducing the transport duration and reducing the stock size and associated cost.



Visible Supply Chain Insight

Global statistics

Transporter profiling

What the project targets with a sufficient value to finance it (build+run)

In most of the case, nothing is done here, and value is lost

Let’s make a short break

LEARNING AT THIS STEP

IoT has recurring costs

Longer the service is delivered, higher the cost is per device.

Business model includes recuring cost

In the initial price (device will have a programmed obsolescence) or within a subscription

Multi-side business can be a solution

By targeting different market and extracting more value from the data you can balance the recurring cost issue

IoT is an opportunity to innovate like Internet or smartphones transformed our environment

Adding a connectivity feature on an existing things does not make innovation happen.

Innovation transforms an existing market or create new markets

IoT changes the way a simple product is produced, distributed, sold…

… more than it is changing the way to use it

- Understand the use of product
- Propose renewal right on time
- Propose maintenance based on use
- Per use billing
- Unlock special blade
- Allow opening
- Track product in distribution circuit
- Fight against counterfeiting

Why connecting tables ?

- Would it be for the end-user to master its dinner habits ?
  - Are your ready to pay for it ? **NO !**
- Would it be for the manufacturing process ?
  - Can we save money ? **YES !**

Manufacturers needs to forecast future order with accuracy to plan raw material purchase and flatten manufacturing process.

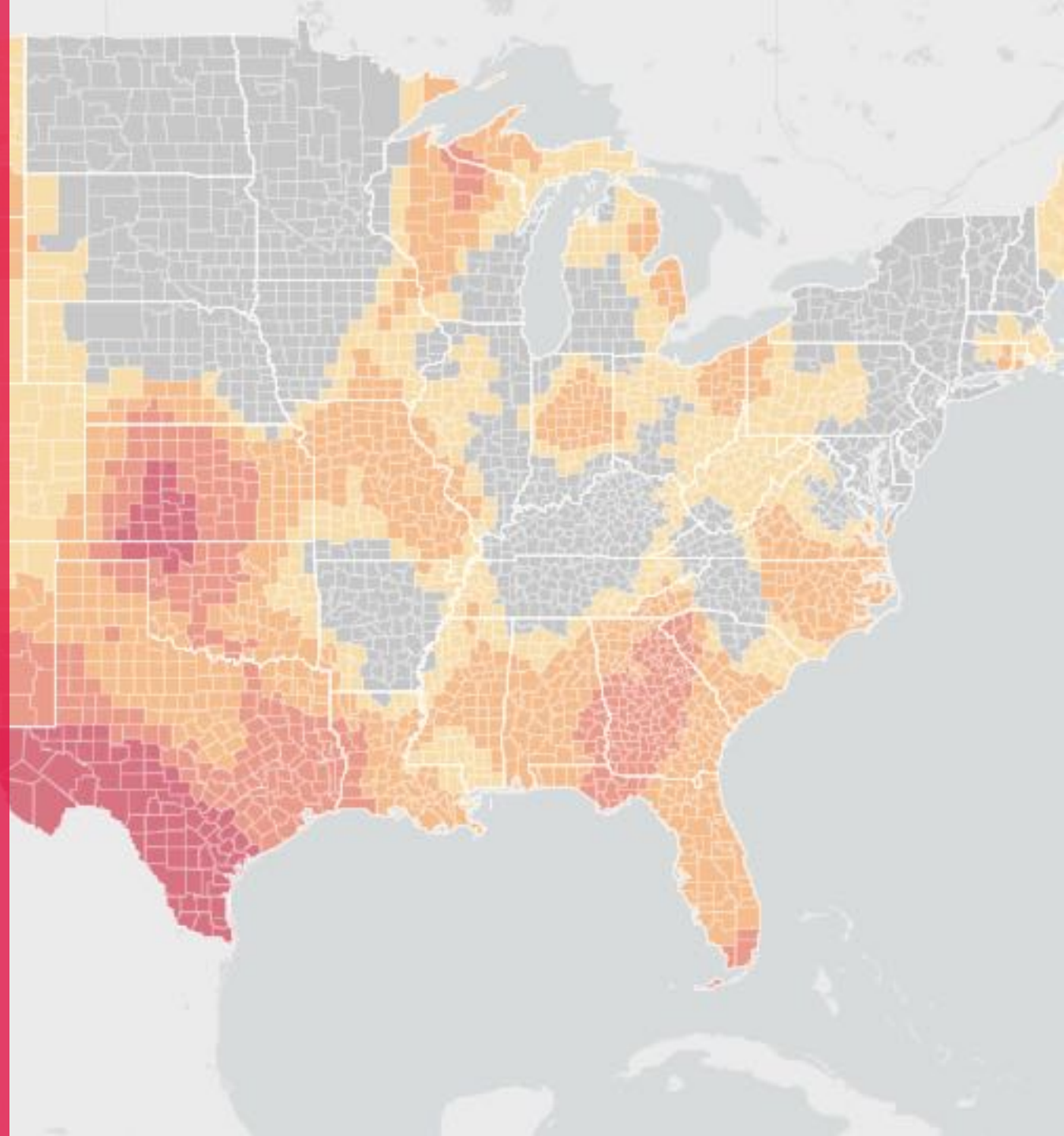
IoT can give them a real time view of the distribution stocks and move away from forecast to real-time market data.

IoT can fight against pandemics

Here is a Map of Covid evolution within the USA made by Kinsa connected thermometer. This is precious visualization obtained with $30-$50 thermometers, complex to use. It is like a satellite watching hearth with a 100km x 100km definition.

How this could be with IoT at Scale providing a 100m x 100m definition, thanks to $3 connected thermometers ?

- It could predict any pandemic movements.
- Gives immediate results even before test.
- It could give transparency all over the world.
- Allow to confine small area instead of whole countries.
- It could protect the personal data more than the existing solutions.



IoT for public led problem to service

Public lights are fails and detection is usually made manually on regular basis.

- It has a detection cost
- It implies a bad quality of service

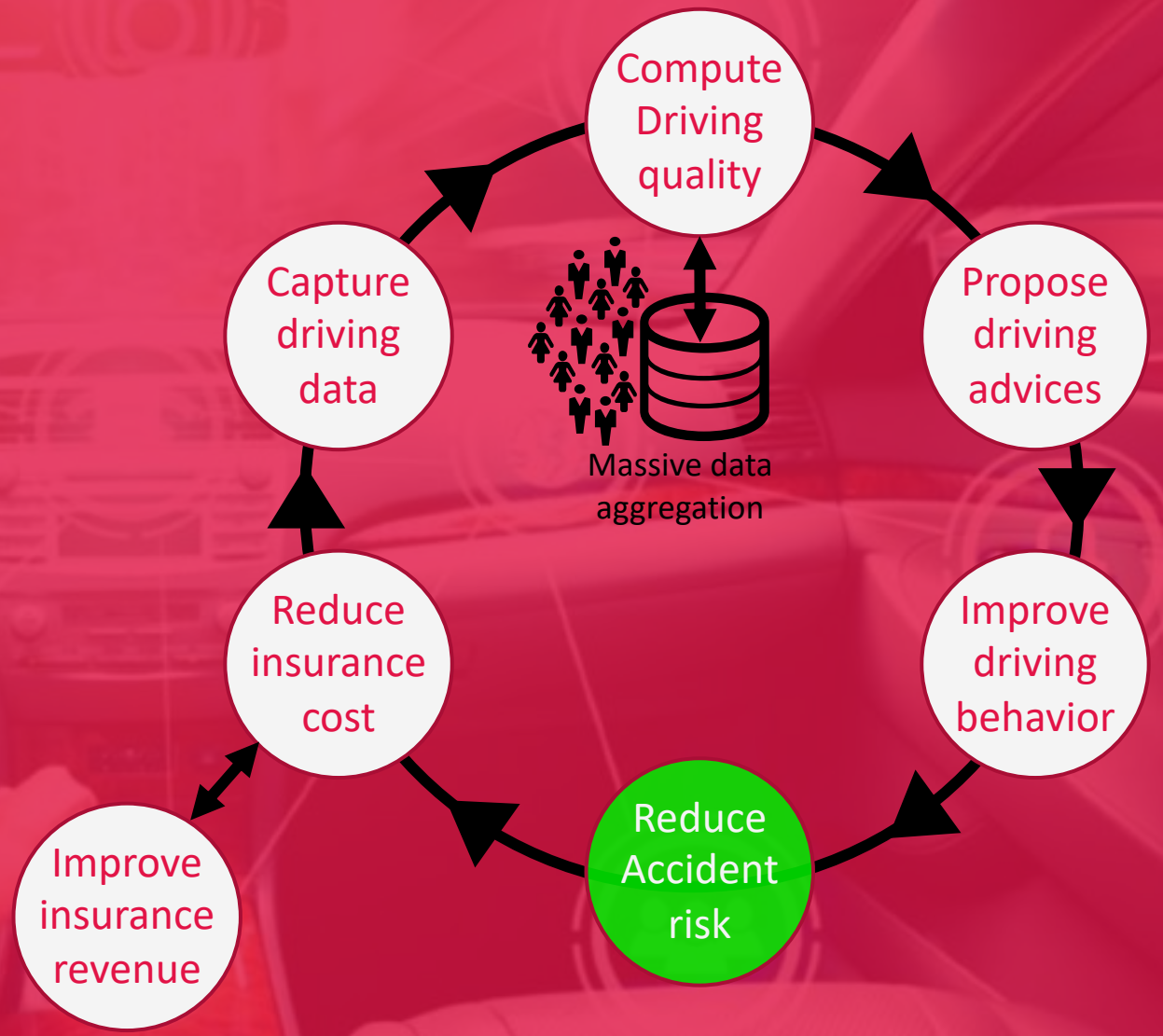
Connected lights can reduce the detection cost, allow to get an immediate detection and maintenance offering a high quality of service.

But it is also an opportunity to transform this kind of maintenance as a service, being able to do predictive maintenance.

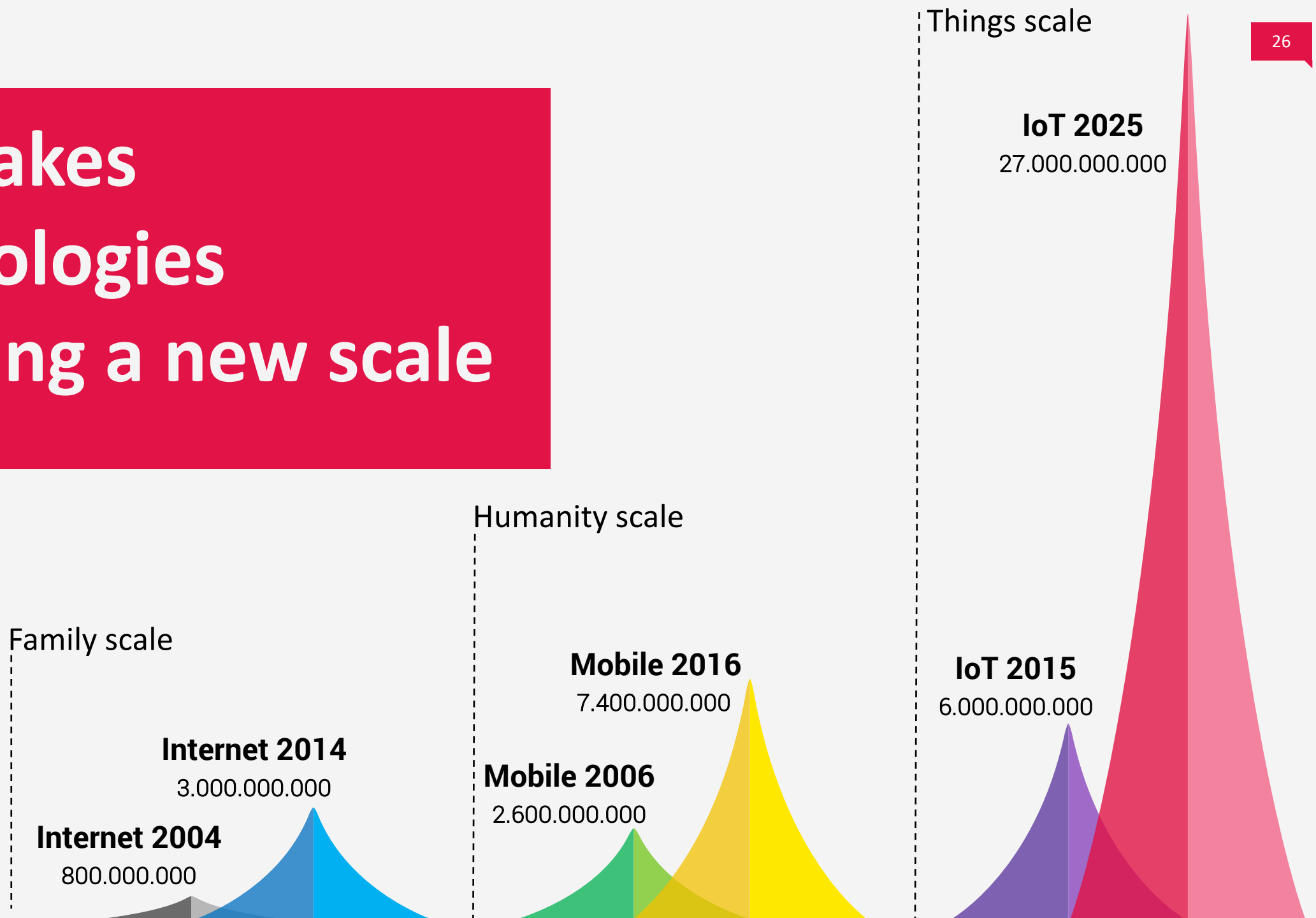
It’s also an opportunity to change the way the city lights are managed and to save a lot of energy with a higher service level for the citizens.

Connecting a light today is less than $2 hardware.

IoT for safer mobility



IoT makes technologies reaching a new scale



IoT at scale

What makes the difference and innovation with IoT is the ability to **make it at scale**. The ability to **deploy millions of devices in the field**.

$1

ULTRA-LOW-COST DEVICES

In 2020 we reached under $1 IoT devices firs condition to support at scale deployment

IN FIELD COST TENDING TO ZERO

The second condition to support at scale deployments.

IoT as the source of physical world AI

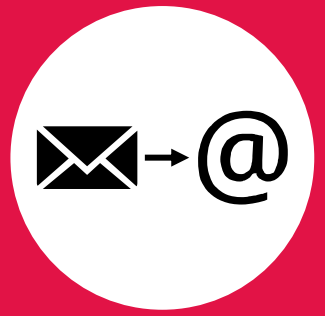
IoT CAPTURES THE ENVIRONMENTAL DATA
DATA FEED THE AI.

AI main domains of implementation **is digital world** (images, video, sounds, voice, social network, books …)
The AI capabilities in the physical world is huge (car driving, industrial maintenance, pollution, energy consumption reduction, climate prediction, health & pandemic…)

Currently, **physical world AI** is limited by the small number of data we have for training the neuronal networks.
IoT, by massively gathering physical world data **is enabling new AI capabilities**.

Let’s make a short break

LEARNING AT THIS STEP



IoT is transforming a market

Making things communicating, automate reporting is not enough

It allows to get data from Things anywhere

It gives the solution provider to grab data from any of the things at scale

IoT scale is Things scale

IoT revolution will make sense at scale, therefore the most important things for a breakthrough is the solution TCO per Things

IoT have multiple faces for addressing all the Thing's contexts.

New networks made IoT to come alive.

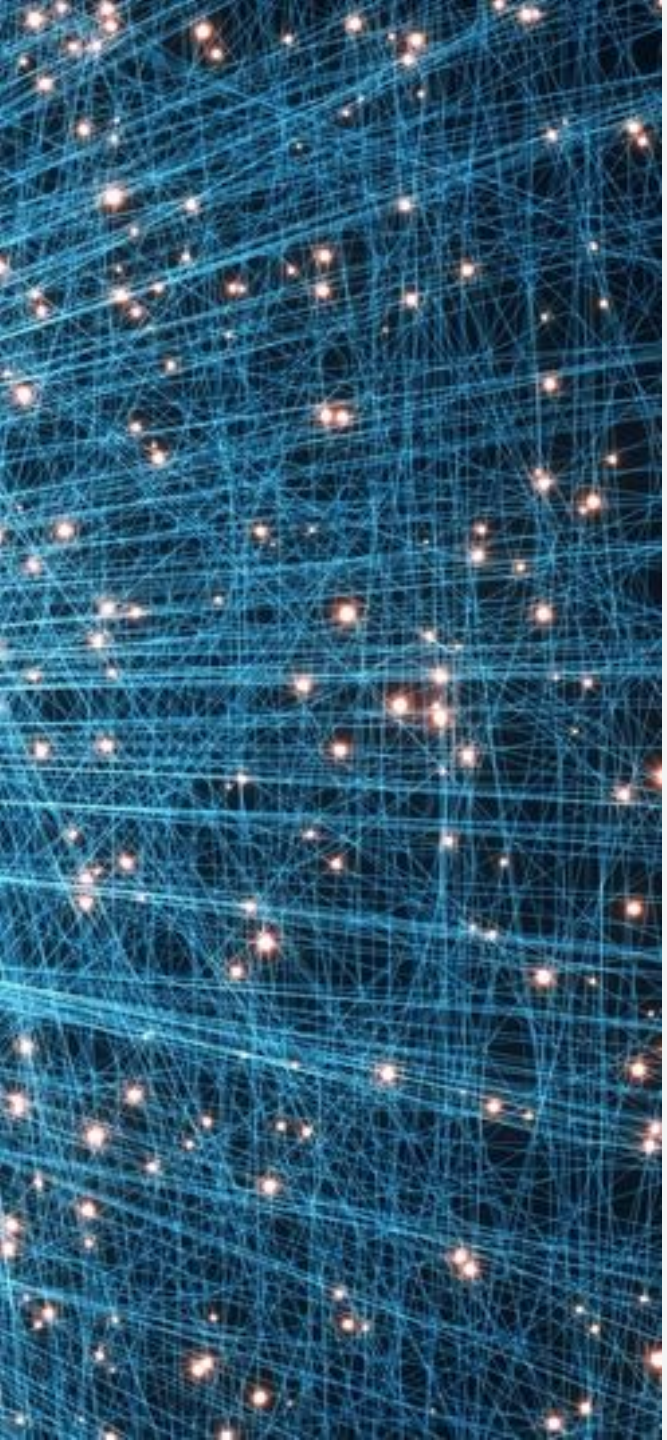
Wearable – human data capture

- 1 day to 1-week autonomy
- Small
- Not expensive
- Subscription challenge

- Get benefit of the human smartphone
- 5m coverage
- Free large bandwidth*

- Focus on user experience
- Belongs on personal data

* This perspective is a market size limiter…



Network characteristics for

Wearables

BLUETOOTH

For customers with a smartphone AND data.

This is basically limiting the target population

Target Geeks

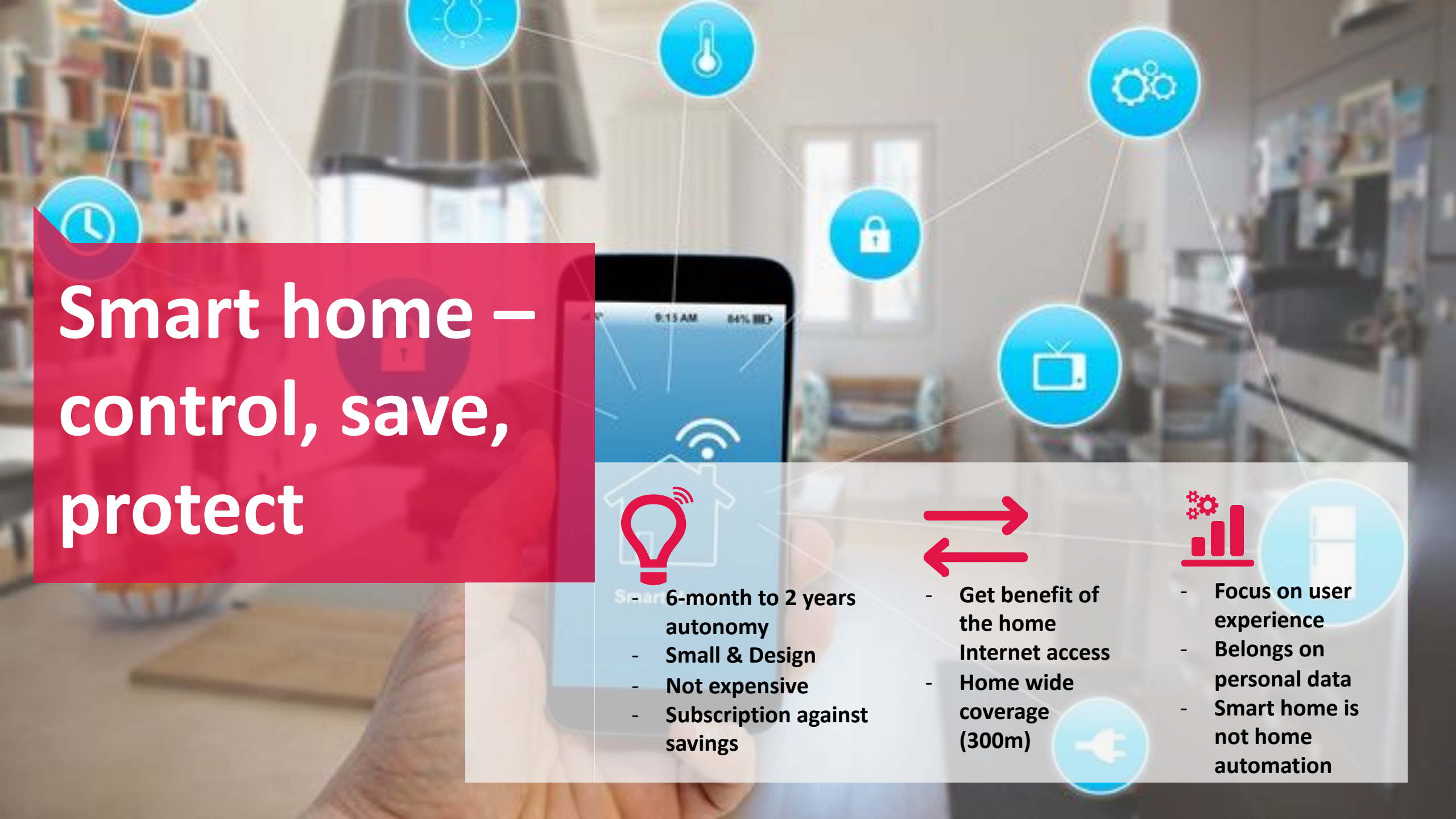
CELULAR TECHNOLOGIES

Enable access for all with a constraints on communication costs

Reduce autonomy

Target elderly, non geeks

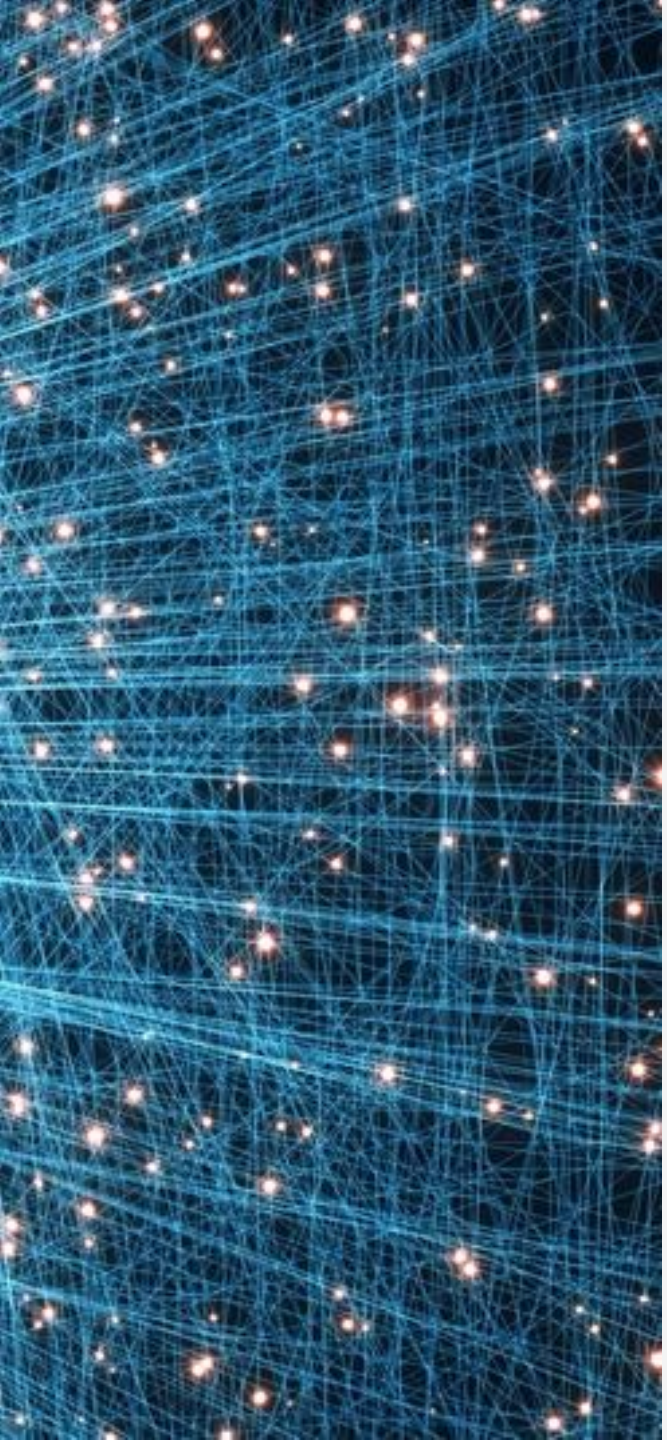
Smart home – control, save, protect



- 6-month to 2 years autonomy
- Small & Design
- Not expensive
- Subscription against savings

- Get benefit of the home Internet access
- Home wide coverage (300m)

- Focus on user experience
- Belongs on personal data
- Smart home is not home automation



Network characteristics for

Smart Home

ZIGBEE

With a gateway connected to home Internet

Low energy communication solution including mesh capabilities

WiFi

Already existing every-where with coverage limitation.

Configuration is complex

LoRa

With a gateway connected to home Internet

Low energy communication solution with large coverage

Bluetooth

With a gateway connected to home Internet

Mesh or long range for smart home. Easy to connect with smartphone

Smart city – optimize, greenify…

- 5-years to 30 years autonomy
- No maintenance

- Low cost
- Small bandwidth
- City wide network (10 - 100km)

- High level of insight
- Massive data processing
- Money/Energy saving oriented
- Subscription

Network characteristics for

Smart Cities

0G

LoRaWan

Low power network easy to deploy city-wide as private.

Easy to share between multiple project.

Flat cost

Sigfox

Public World-Wide Low power network already covering cities.

No deployment and maintenance cost but subscription Ultra low-cost devices

4G

Existing technology is most of the cities, allows large traffic but energy consuming.

LTE-M and NB-IoT low power but still limited

5G

To be technology coming with valuable power efficient solution with large bandwidth compared to 0G.

Subscription based

MESHED NETWORK

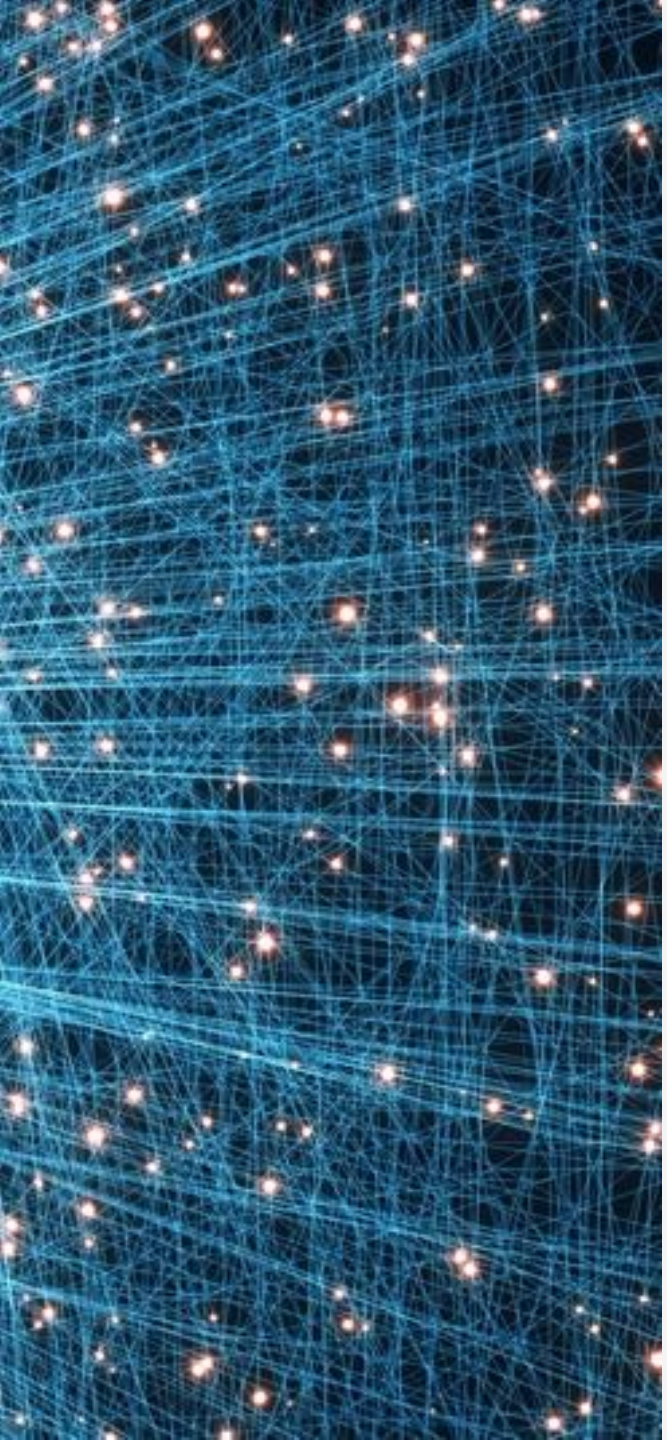
City wide meshed network like Amazon Sidewalk are promising for B2C and could be used for Smart Cities

Industrial IoT – reduce costs, improve quality, secure investments

- 1-years to 30 years autonomy
- Reduced maintenance

- Take benefit of existing networks (M2M)
- Autonomous in private network (or public)

- Difficulty on multi-tenant added value.
- Massive data processing
- Money/Energy saving/Risk reduction oriented



Network characteristics for

Industrial IoT

ETHERNET

Old M2M technology already in place.

Reliable and secured but costly for massive deployment

Reduced maintenance, not mobile

WiFi

Already in most of factories and warehouse

Configuration is complex

Reduced autonomy

LoRaWAN

Allows to deploy private network at low cost.

Industrial site coverage with 1-3 gateways only.
Reduced maintenance

Long Autonomy

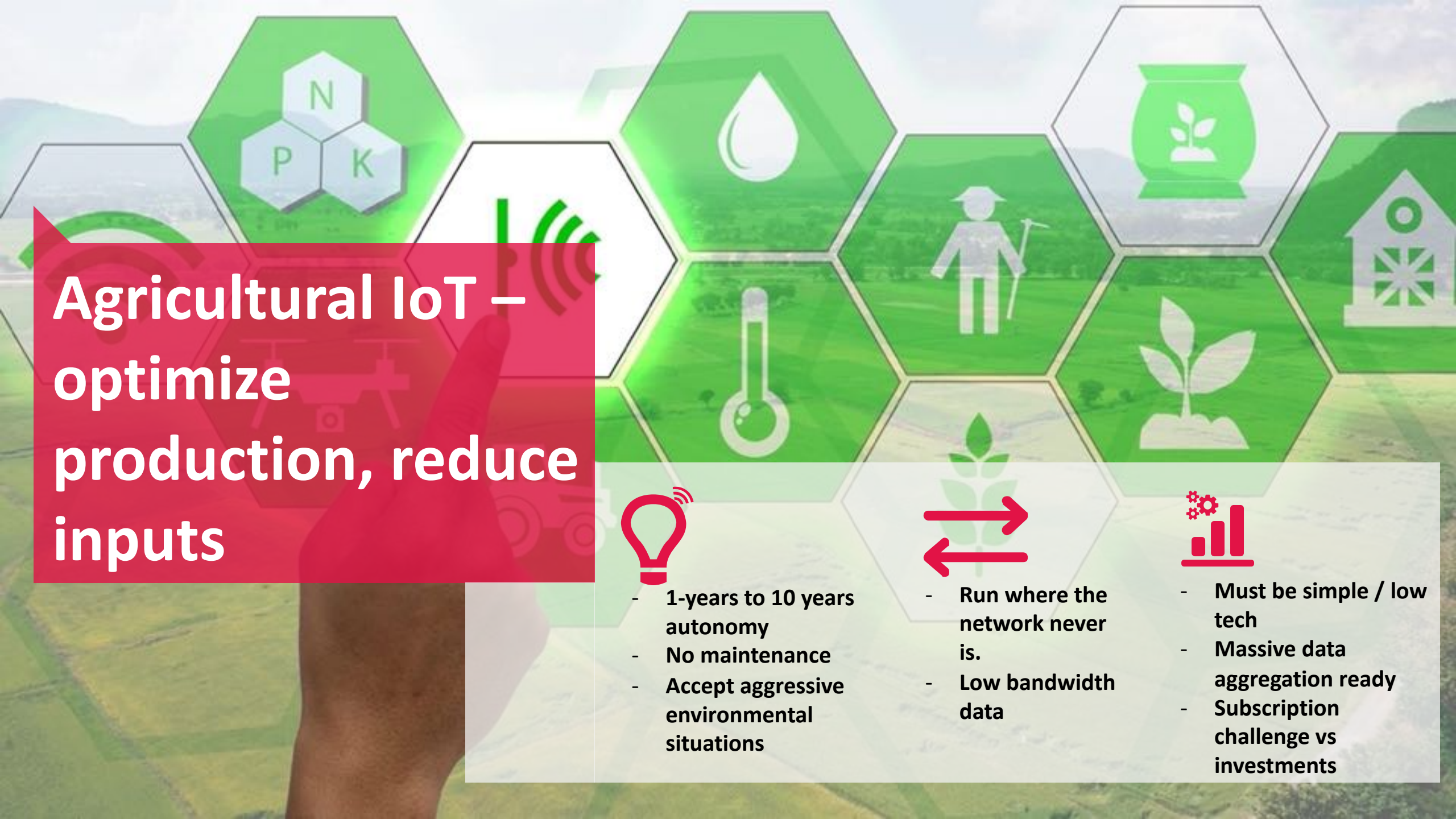
Sigfox

No investment, public network can be extended locally.

No maintenance cost, subscription cost.

Long Autonomy
Ultra low-cost devices

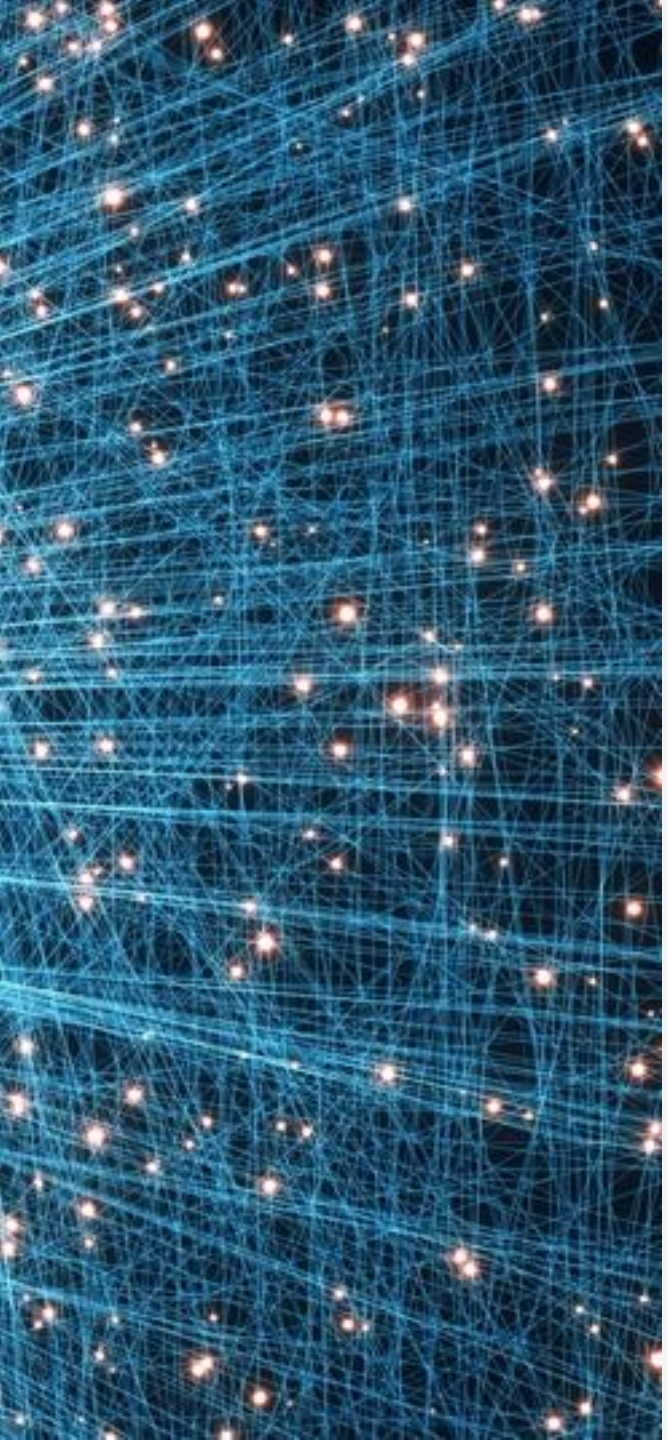
Agricultural IoT – optimize production, reduce inputs



- 1-years to 10 years autonomy
- No maintenance
- Accept aggressive environmental situations

- Run where the network never is.
- Low bandwidth data

- Must be simple / low tech
- Massive data aggregation ready
- Subscription challenge vs investments



Network characteristics for

Agricultural IoT

CELULAR

Usually deployed far after cities, country-side will mostly rely on 2G / 4G technologies.

Allows when needed large data transfer

LoRaWAN

Allows to deploy private network at low cost.

Agricultural site coverage with 1-5 gateways only. Reduced maintenance

Long Autonomy

Sigfox

No investment, public network can be extended locally.

No maintenance cost, subscription cost.

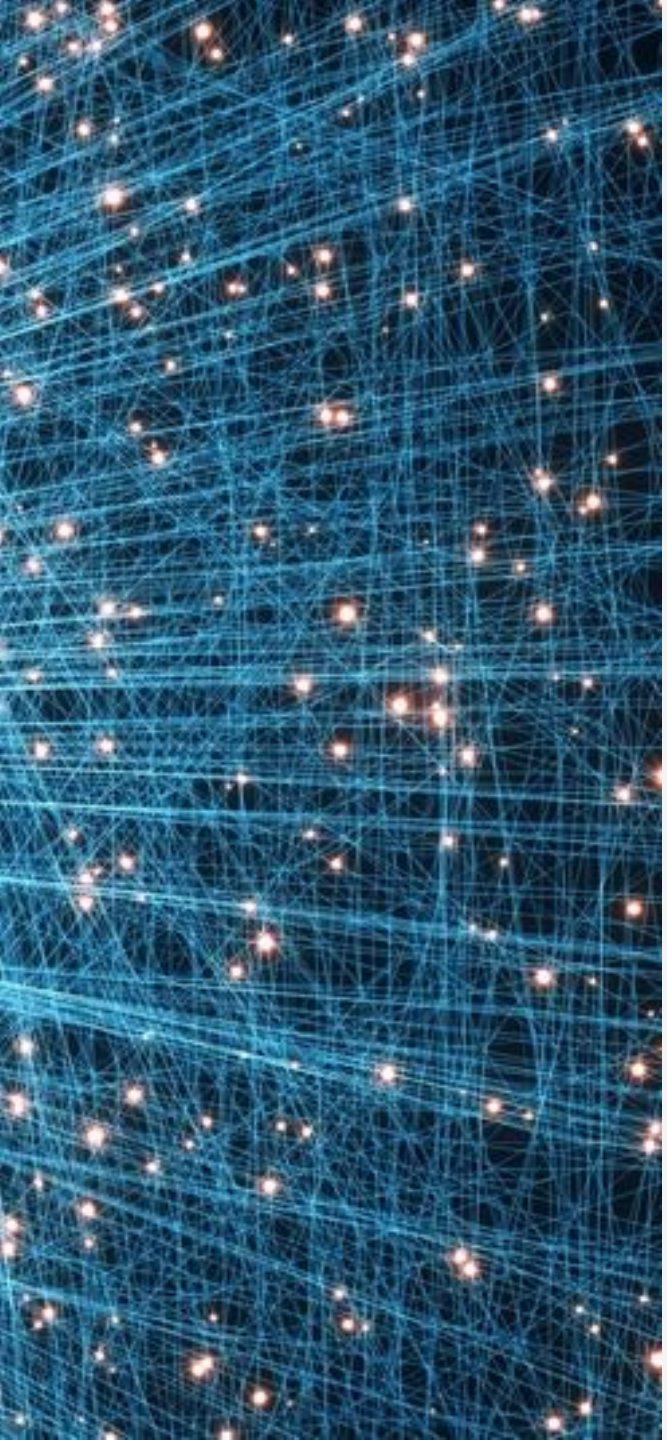
Long Autonomy
Ultra low-cost devices

Supply chain / Logistic IoT – optimize, track

- 1-years to 3 years autonomy
- Low maintenance
- Low cost
- Vs Precision dilemma

- Nation-wide to world-wide
- Low bandwidth data

- Cost challenge
- Integration challenge
- Multiplicity of solution providers
- From the truck to the things.



Network characteristics for

Supply & Logistic IoT

CELULAR

Need world-wide coverage, well deployed networks.

4G, sometime 4G LTE-M with fallback.

Energy consuming but having a large historical footprint

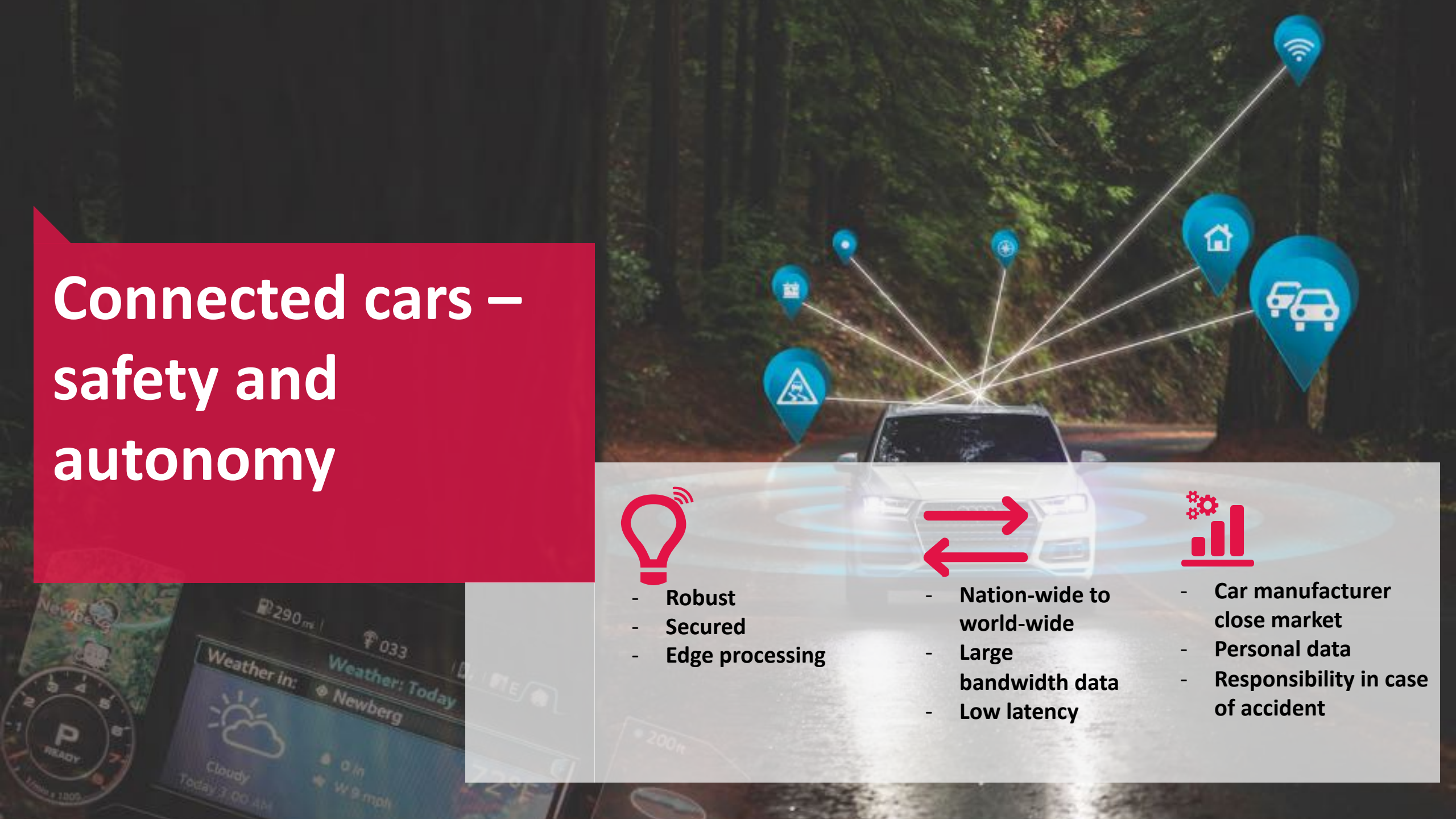
Sigfox

The growing network covering many countries as a single one.

Simple to use. Low power consumption

Ultra Low Cost

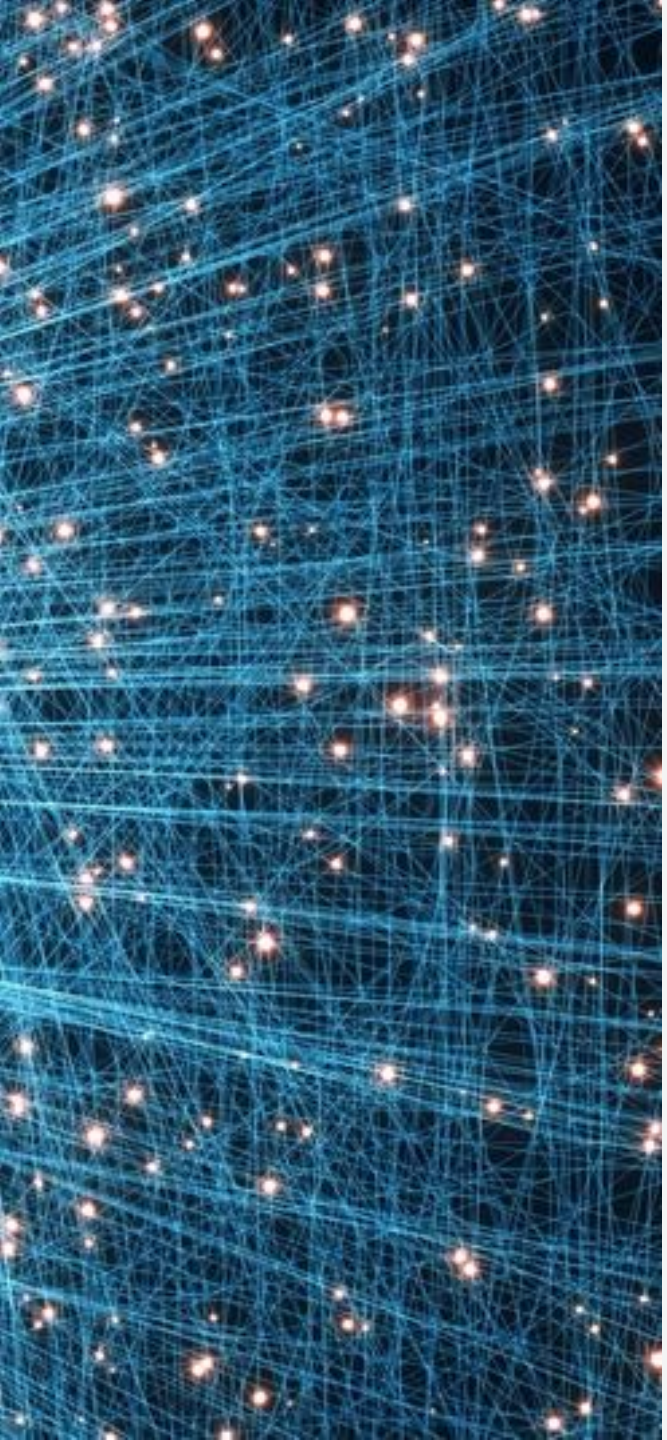
Connected cars – safety and autonomy



- Robust
- Secured
- Edge processing

- Nation-wide to world-wide
- Large bandwidth data
- Low latency

- Car manufacturer close market
- Personal data
- Responsibility in case of accident



Network characteristics for

Connected cars

4G

For the next 5 to 10 years the networks will remain 4G in certain area.

5G

With low latency the 5G will improve autonomous vehicle by connecting cars each others.

Let’s make a short break

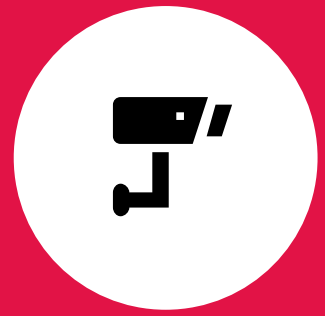
LEARNING AT THIS STEP

IoT has many faces

There is not one IoT but different domains where IoT applies with different targets, different constraints

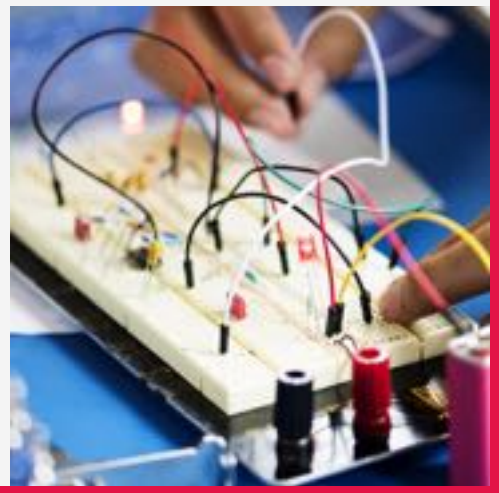
Many technologies are covering these faces

To solve the different constraints, we have a large set of technologies. IoT revolution comes with the arrival with these technologies as enablers



Data access vary

Depending on the execution context, data sensitivity vary and the ability to manipulate it of makes added value with massification vary.



What is an IoT project ? Main steps, technologies involved, associated investments

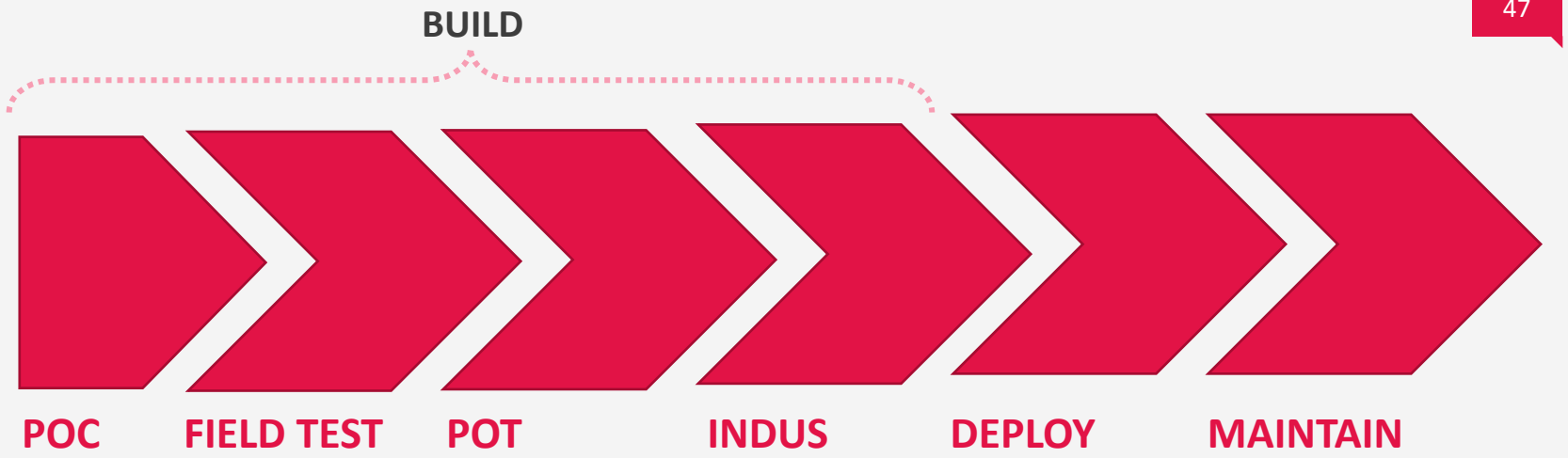
Typical IoT Project timeline

Successful IoT projects are the one getting the best Field experience in the early stages.

Do not make the large investment needed in the industrialization phase until making them.

18 **Months – usual duration for an IoT build project**

80 **% Share of build investment spent in INDUS Phase**



Create the final product, create the associated platform and UI

Fix the technologies and make small batch of the future design solution. Ensure it respects the constraints.

Answer a single question - with a deployment limited to 5 to 20 devices, raw data captured and simple excel like analysis – Would we reach the expected business value creation ? The tech team will also get benefit of this field experience.

In days or week, using market available bricks for hardware and software. Network solution should be identified. Cost of the solution, autonomy, UI have nothing to see with future solution.

2-3 weeks timed-boxed

1 POC phase

Create a quick & dirty solution able to determine the main fields issues solution, get the first set of data and prove the business model ; imagine business model extension.
We are using out of the box building blocks.

AIM ON THE FASTEST

Autonomy, cost, size, design are not the problem to solve at this step. Use existing elements, buy/hack existing devices. Multiply sensors, use local storage if needed.

SELECT THE RIGHT NETWORK

Network will be a major field constraint impacting the business model. It's better but not mandatory to select the right one.

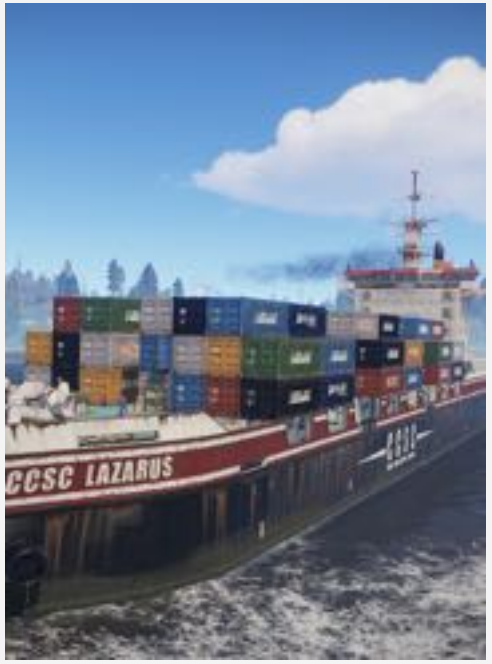
USE OF MARKET IOT PLAFORM

Do not invest on UI, Excel is good enough, but there are many IoT platform on the market you can connect your prototypes.

10-30 weeks

2 Field test

Deploy 20 to 100 POC devices on the field, in the real conditions, measuring the expected data + a maximum of environmental data. You need to be sure to understand the input impacting the business model.



ACCEPT TO LOST DEVICES

Any destroyed device is an opportunity to understand an unexpected situation. Ensure you have a diversity of context corresponding to the target situations.

VERIFY YOU CHOICE VIABILITY

Identify reasons of communication loss. Analyze each of the situations.

AT-SCALE, BEYONG THE HORIZON

Any captured data is analyzed, imagine what you can get from at-scale data-set. Find the right frequency / energy / precision balance. Look at un-expected use and potential new business transformation of business models…

10-30 weeks

3 POT phase

Design a device with the targeted technologies, supporting the fields constraints, with the expected autonomy, cost compliant … Automate the main identified Insight generation.

VERIFY TECHNICAL ASUMPTIONS

Small batch of devices, logging information and environmental information but like production expectation. Identify future production constraints and respect of fields constraints. Source different chip providers and start to negotiate price & volumes.

VERIFY YOU CHOICE VIABILITY

Continue the test field, start negotiate the subscription with the network providers…

CONFIRM VALUE CREATION

With a larger historical set of data and a larger number of device, confirm your value proposal. Start looking at indirect market you could reached, start contacting potential customers.

30-80 weeks

4 INDUS phase

Create the solution: the product with a mass production capability, including test, packaging… Create the application and all what is needed to deploy and maintain the solution.

PRODUCE AT SCALE

Design the product for being made at scale. Electronic, mechanic, assembly, test automation, certifications, patents… This step requires a huge dose of engineering, with potential innovation.

INTEGRATE WITH SERVICE PROVIDER

You need to automate the subscription process, subscription renewal and subscription cancelation

BUILD THE APPLICATIONS

You need to build the entire platform plus the different rendering applications. You can have Insight but also mobile application, websites … This is mostly classical IT but many things need to be built. Do not forget to include device life-cycle management.

Application

FROM POC TO DEPLOY

POC Raspberry PI with custom made shield for radio transmissions

POT Device with target technology & sensors

POT2 Device with target technology, sensors and target design approach

Pivot 1
Behavior is different
From global a platform to a dedicated device

Pivot 2
Design is different
From a commodity to a designed device

MYTEEPI

Industrialized product.
Ready for batch production
@ 1000 units

Evolution of a product from the POC to the DEPLOY

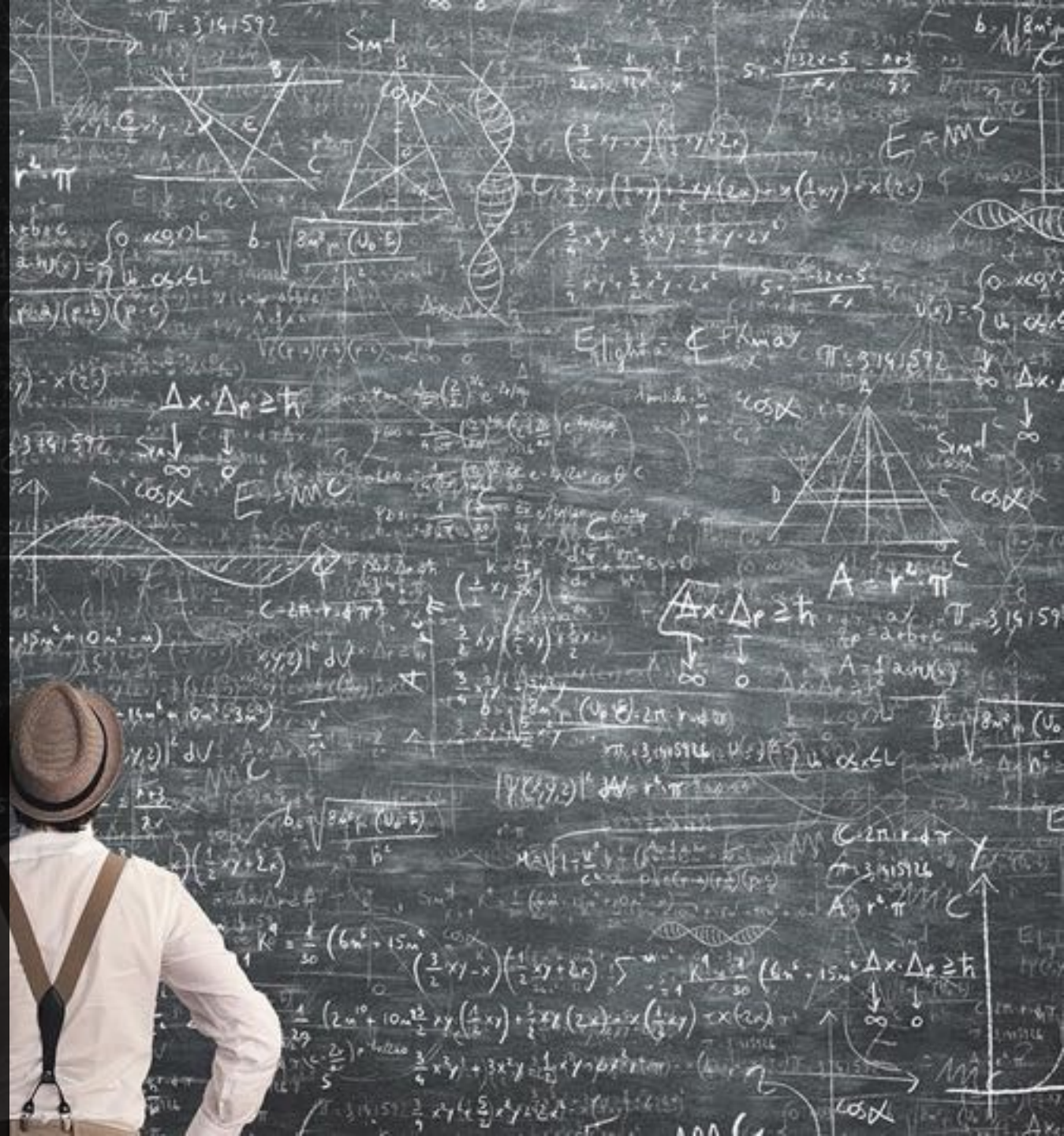
An IoT Project is a complex Project

It can be managed in an Agile approach to get deliverables more frequently, but never consider it as a simple IT project, it's much more complex. Complexity depends on:

DEPLOYMENT SCALE
Making 10 devices will not be the same as 1M

SIZE OF YOUR COMPANY
This is in relation with the risk level you accept to take and the investment you can support

THE GEOGRAPHICAL SCOPE
Hardware deployment requires certification, certifications are made per zones. Technology availability also differ per zone.

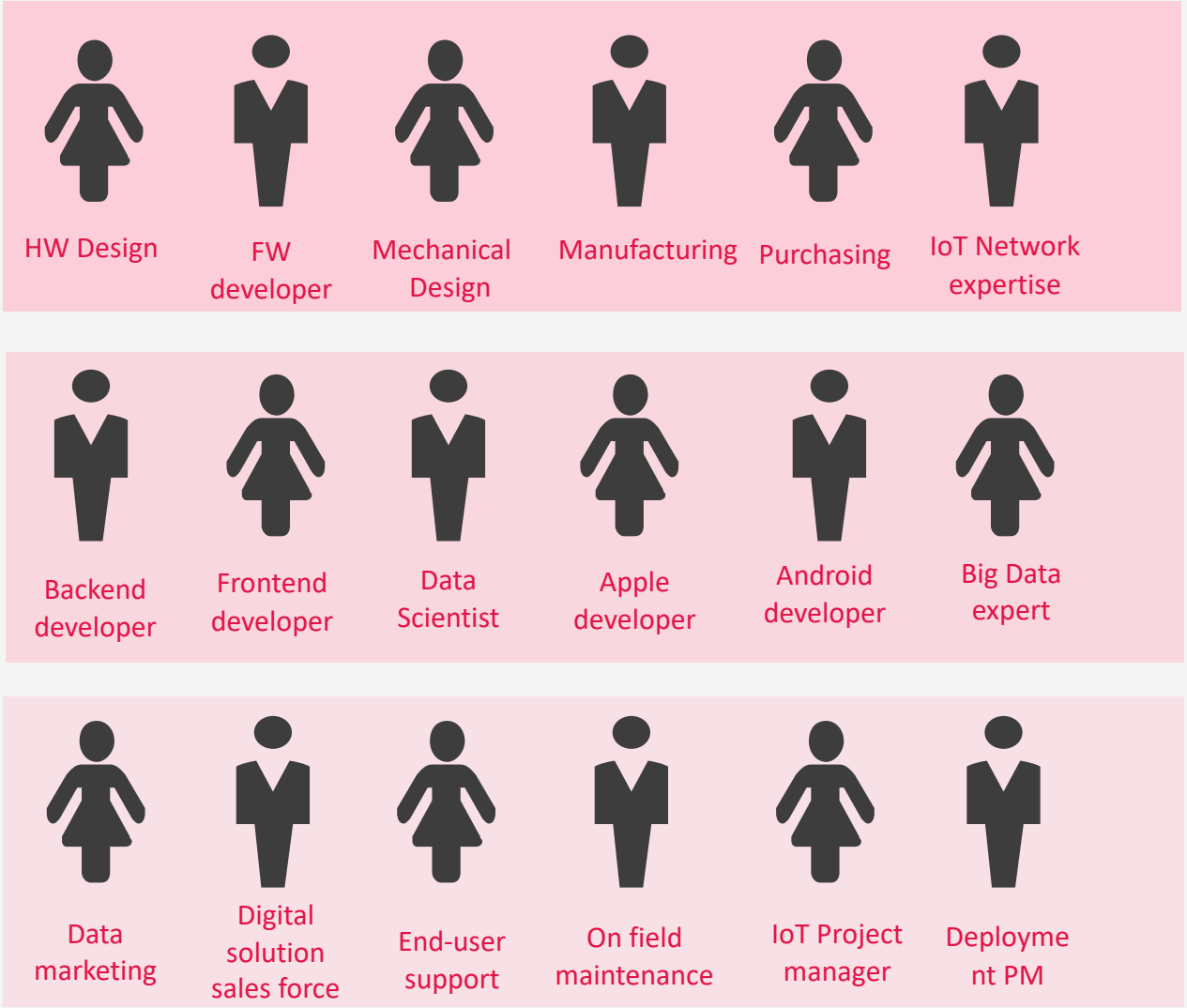


Typical IoT Project team

IoT requires a lot of different expertise You can't expect to find in your existing teams if you're not already an IoT company.

These skill are far away from the one you find in a furniture industry. This is a problem for the IoT transformation.

This problem is bigger than in the digital transformation.



All these expertise are rare and far enough apart that no one has more than 2

IoT is also a question of choice and compromises

Due to the physical world, hardware design and particularly IoT where size, autonomy and price are key elements, you need to makes some compromised on your initial expectations otherwise, the experience is, you will never start your project.

All the directions on the right schema are antagonists

Let’s make a short break

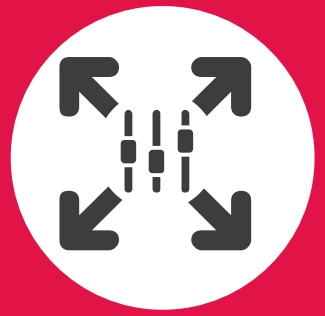
LEARNING AT THIS STEP

IoT projects are complex

You can make a PoC in a few week but you must not expect the project to be live in a month.

IoT projects needs rare skills

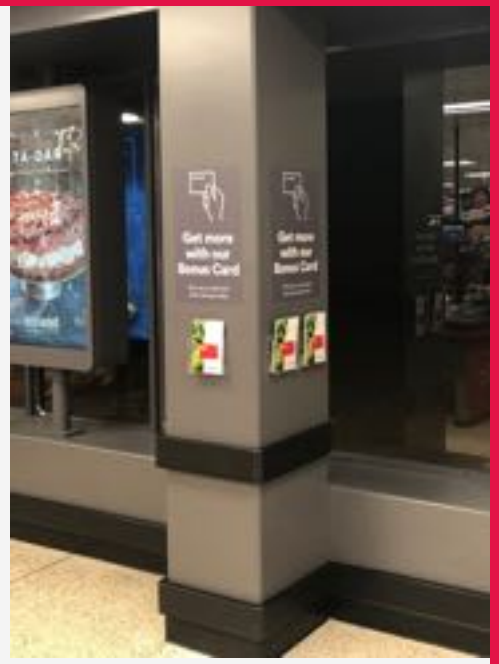
Many different rare skills are needed. This Is a reason why today most of IoT is tech oriented when it should address Things.



Compromises are necessary

There are so much constraints in an IoT project that you need to accept compromises. The key factor of success need to correctly be established at the early stages.

Marketing & communication IoT use-cases



Yes it is Digital content

Vinyl disk with additional content you can access through a Near Field Contact (NFC).
Create a new end-user experience, mix digital and analogical content and sound.

By adding an ID to any physical device and making it accessible with a Smartphone, you can create a new consumer experience.
It also works for restaurants, bar, hotel… make a quick & easy access to additional services in a simple way.
Business model : loyalty and premium services

PASSIV DEVICE

No maintenance, no end-of-life. No dara.

BASED ON NFC

NFC is just an ID authenticating the product.

BACKEND CONTENT

Extend the experience, protect against copy. **What is the business model (no extra revenue)?**

Amazon dash button

Place a re-ordering request just by pressing a single button. It has been stopped by Amazon, here are some of the reasons:

- Cost > 5€
- Complex to setup with a smart phone.
- Alexa could do it.

These issues are fixed by LPWAN and ultra-low-cost: you can imagine the product package automatically detecting its level and reordering by itself.

Amazon is deploying Sidewalk, such devices could be back that way.

Business model: commercial lead.

Low cost device

Cost supported by the brand.

Expose a brand

RELY ON BLUETOOTH

Complex setup with the smartphone

LEAD MANAGMENT

Each of the click is generating an Amazon automatic order

Rover call to action

Rover sent a marketing campaign to 5000 consumers. The user was pushed to click a button to request a car test drive. The response rate has been 48% compared to the usual 5%.

The ecological impact is large vs the efficiency. You can detect the marketing content opening and interaction to place the right call at the right time and get a better conversion rate.

Business model: commercial lead.

Low cost device

As part of a global marketing costs

RELY ON SIGFOX

No settings, just work. But subscription model is a problem currently

LEAD MANAGMENT

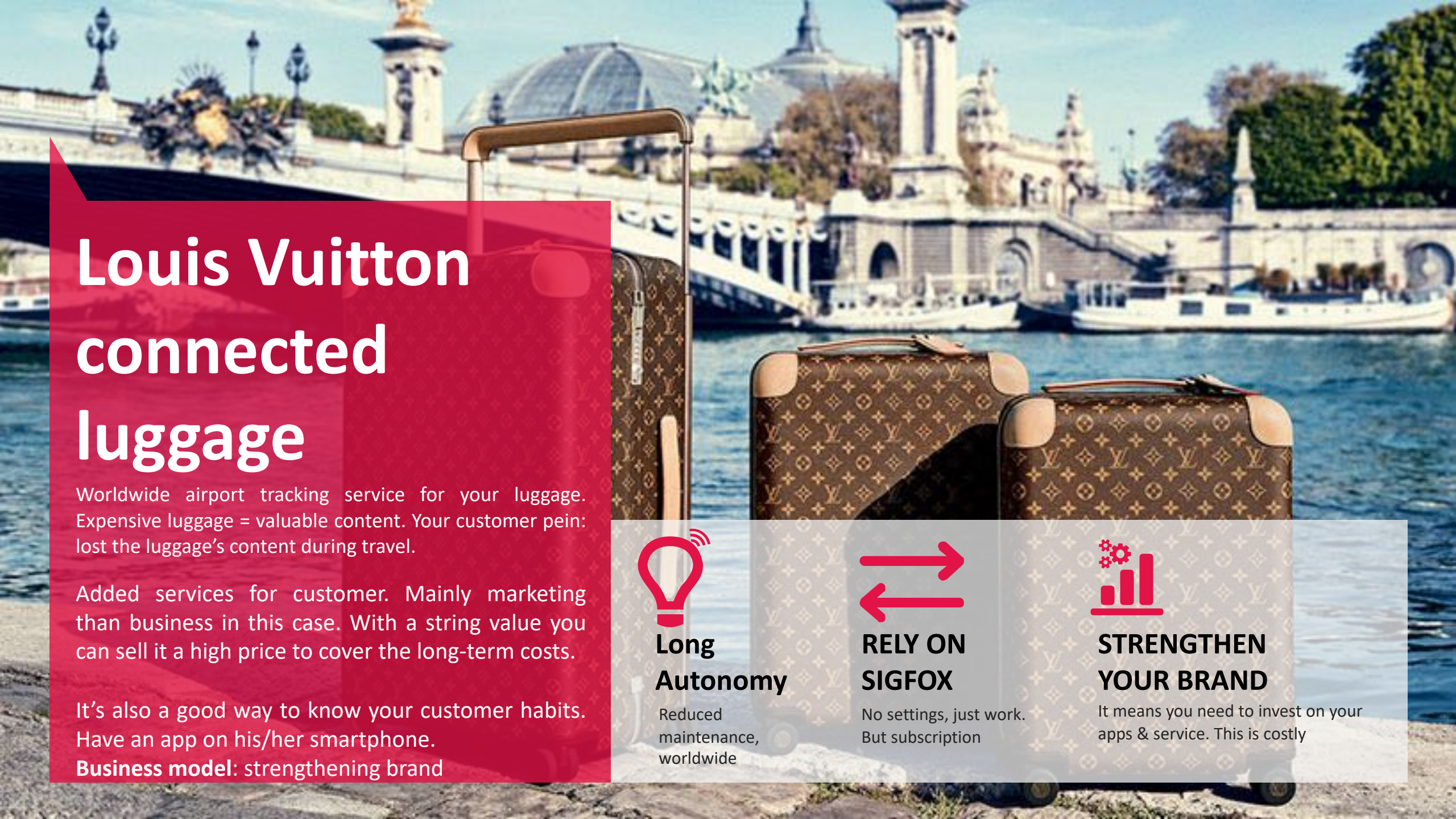
One shot operation. No long-term cost to support

Louis Vuitton connected luggage

Worldwide airport tracking service for your luggage. Expensive luggage = valuable content. Your customer pein: lost the luggage's content during travel.

Added services for customer. Mainly marketing than business in this case. With a string value you can sell it a high price to cover the long-term costs.

It's also a good way to know your customer habits. Have an app on his/her smartphone.
Business model: strengthening brand



Long Autonomy

Reduced maintenance, worldwide

RELY ON SIGFOX

No settings, just work. But subscription

STRENGTHEN YOUR BRAND

It means you need to invest on your apps & service. This is costly

Brand protection

A digital product comes with an application. You can make sure of the source of the digital product when in a purely physical product you can get a perfect copy requiring expertise.

As a brand, you can certify your product origin, your customer will be sure of the provenance. You can also force the copied application to be removed from app marketplaces because they are centralized. This is more difficult with manufactured product make in country where you have no legal level to close the factories.

Business model: protect your brand and future revenues.

Long life duration

Because toys lifecycles are really long

BLUETOOTH

For smartphone integration

LOYALTY AND BRAND PROTECTION

Long life of application with no subscription model. Brand investment more than money making. High quality is required.

Contact tracing

In case of pandemic, IoT allows a massive contact tracing with a high level of privacy compared to cell-phone solutions.

IoT contact tracing can be massively deployed at low cost with no technological requirement compared to smartphone solutions.
The reliability of the radio measures is still the hard part with the associated battery autonomy.
In term of data for statistics and propagation model it is really value added.

Business model: state investment / PIB protection

LONG AUTONOMY

Reduced maintenance, no pre-requisites

SIGFOX

Cost, autonomy, no setup, global

AT SCALE, SECURED…

Here the platform criticality is high in term of scalability and data sensitivity for the states

Count strike participant

Number of participants is an important question and the responses from the different sides are usually totally different. Numbers can help to get the truth.

Smartphone density is a good way to count people. The cell tower around and all along the demonstration are capturing the pic of people and the difference with a normal day or a couple of hour before gives a good estimate of the crowed size.

Business model: side use of existing data

DOES NOT GET NOTICED

Meta-data information captured for other purpose

3GPP

Mainly deployed technology

INSIGHT ONLY

This is just insight based on data captured for another service.

Identify, count traffic jam

There are many ways to measure it, on of them is to measure the density of smartphone in a cell-tower area and to measure the time one same smart-phone stays registered to the same cell-tower. Basically its velocity.

This is another example of what we can do with metadata coming from the smartphone networks.

Business model: side use of existing data

DOES NOT GET NOTICED

Meta-data information captured for other purpose

3GPP

Mainly deployed technology

INSIGHT ONLY

This is just insight based on data captured for another service.

Shop, museum frequentation

This information you can easily obtain, in real time, comes from the smartphone you have in your pocket.
Any of you is a bit generating the frequentation reports.

This is a highly valuable information for business size, growth estimation, location value, even fiscal control.

Business model: Insights generation

DOES NOT GET NOTICED

Meta-data information captured for other purpose

3GPP

Mainly deployed technology

INSIGHT ONLY

This is just insight based on data captured for another service. And integrated in multiple services or studies.

Pollutions data

Measure the pollution, accessing to reliable data is a key element to act and control.
There are so many different type of pollution and getting a measure is expensive, so we have not a lot of sensors deployed.

Year after years, we see lower and lower cost sensors. The ability of the crowed to deployed sensors will make transparency higher. It will also improve the data quality and reduce the ability to bypass the rules.

Business model: making a better world

LOW COST

To be able to be crowed sourced or deployed at scale

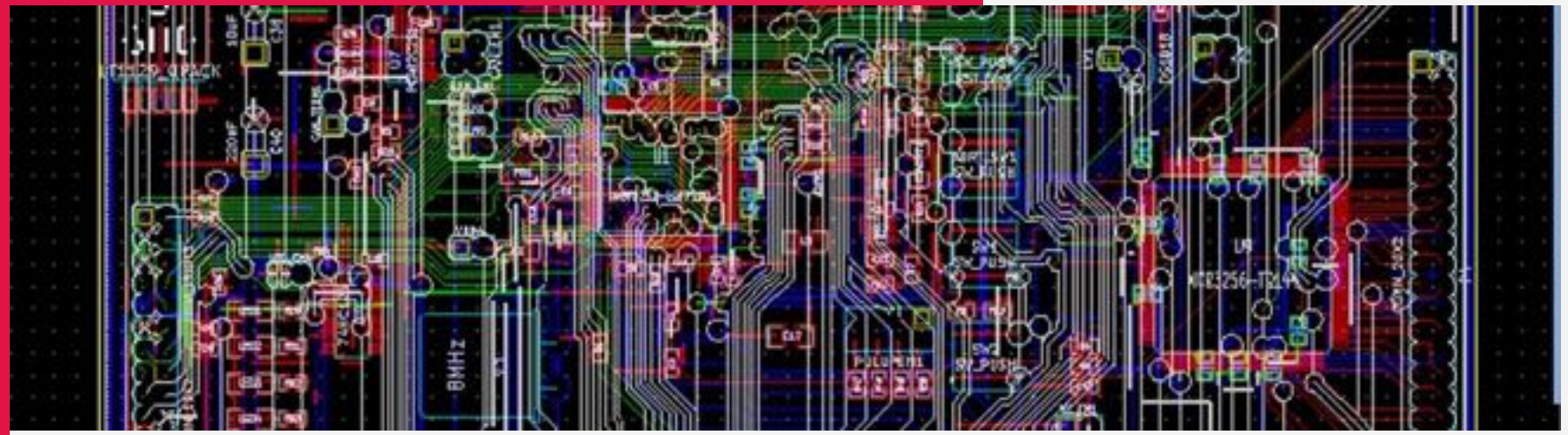
ANY

Depends of the type of device

OPEN DATA

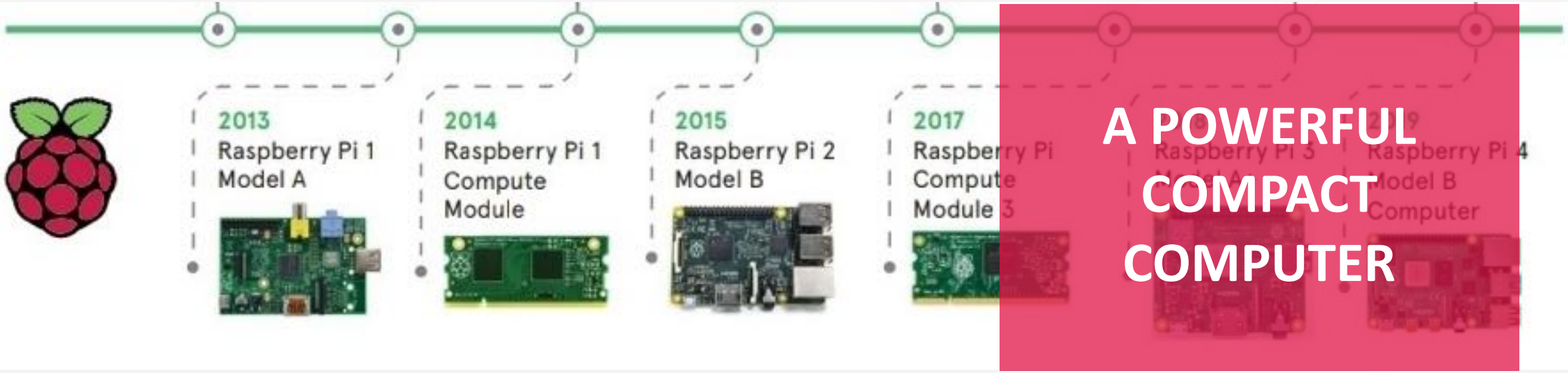
Allows anyone to access these data and use them for make change happen.

What are the main technologies in use to make the devices ?



Device technologies

POC Phase – Raspberry PI



Raspberry PI micro-computers are powerful computers:

- 4 core @ 1.5Ghz
- 2GB to 8GB MEMORY
- WiFi, Bluetooth, Ethernet

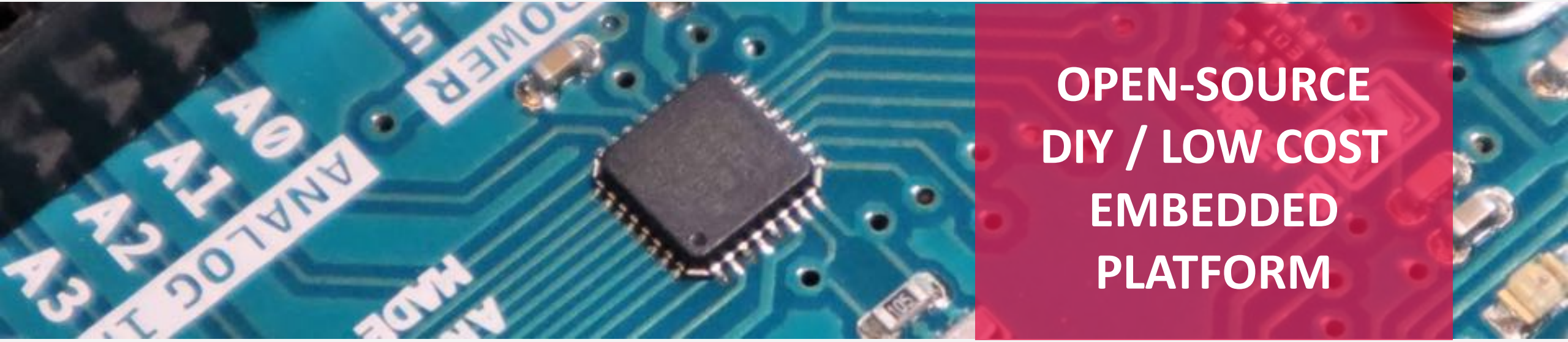
But low-cost: 50€

They are offering an environment to execute high level programing languages like C, Java, Ruby, Go, Perl, Python… with the ability to connected sensors.

They are not power efficient, but you can run them on batteries for day to weeks.

Device technologies

POC Phase – Arduino



OPEN-SOURCE
DIY / LOW COST
EMBEDDED
PLATFORM

Arduino are accessible low-cost & low-power MCU:

- 1 core @ 16-32Mhz
- 2KB to 20KB MEMORY
- SERIAL PORT

But low-cost: 5€

Thanks to the large ecosystem you can make quick & dirty devices having a long autonomy on batteries (month to years) for a reduced unit price.
Many additional shields and compatible boards are available on the market to avoid electronic design in POC.

Device technologies

POC Phase – Best design = no design

The best hardware choice for POC is when you make no hardware

There are plenty of existing devices on the market, basically around 3000-5000 different solutions your can buy and use out-of-the box.
For a PoC phase by using an existing device you save the design time and avoid the risk of field test bad experience due to your inexperience. Standard developers will be more familiar with device API than hardware developments.

Often, the entire IoT solution can be built on already existing devices ! That's the best choice for investment, time to market and risk taken.

Device technologies

POC/POT Phase – 3d design

3D printing and IoT POC and POT phase really works together. For making sample of the device mechanical design as for adapting a packaging to place the electronic circuits, 3D printer solve many IoT designer problems.

This technology is now accessible for less 500€. The main difficulty is to get your engineers able to design what they need of what the project expect.

Competencies for POC Phases – you can rely on IS teams

A corporate software team can manage a POC phase, even with a reduced hardware experience with the listed technology.
They mostly need to get fun with a such project and to have a Hacker mindset.

Having the internal IS team conducting the POC is best. But they need to stop after and let experts (hardware team) conduct the rest of the phases.

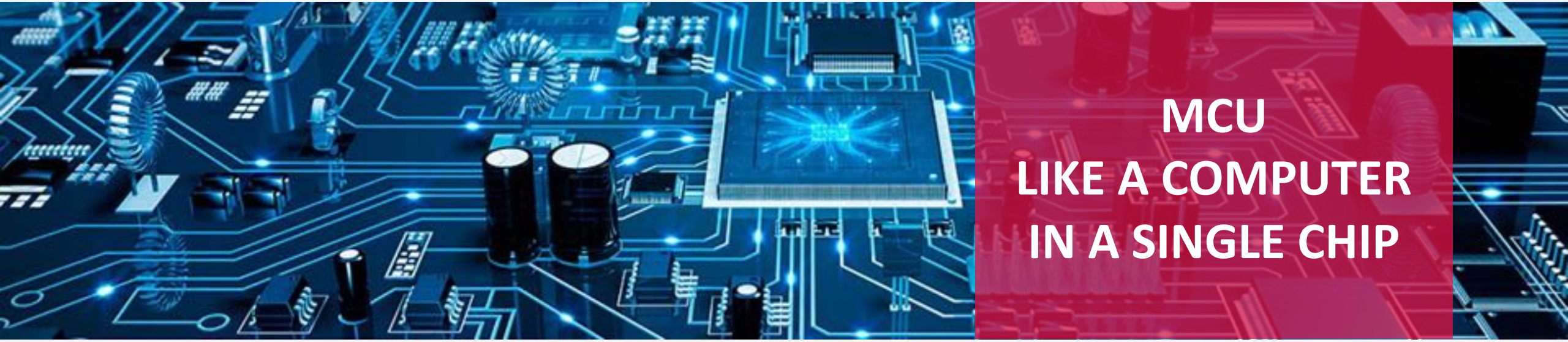
Device technologies

POT – INDUS PHASES

POT and INDUS phase are requiring expertise and a complex work of engineering. If your business is IoT solution, you need to have this team. If IoT is just a solution for improving your regular business, you can rely on an external team. Make sure your have real expert of IoT and not simply a standard electronic design house. IoT is not M2M, there are power consumption, network expertise and IT integration requiring specific knowledge and experience to be successful.

Device technologies

POT – INDUS PHASES - Technologies



IoT Brain is usually a Micro-controller: a single chip containing all what a complete computer have: CPU, memory, storage, I/O ports.
The power of the MCU can exactly fit your device needs and cost only what is needed. Price starts from $0.10 and is usually around $2-$4.
Therefore an electronic design is dedicated to only 1 specific use: each of the components are selected to fit exactly the specific device needs. It reduces the final device cost.

POT – INDUS PHASES - Technologies

Second critical component of an IoT device, the communication circuit. It can be:

- a module, all in one solution, including communication protocol, easy to use, already certified but more expensive ($3-$15)
- A SiP or SoC, they are module made a different ways, more compact but equivalent.
- A transceiver, this is the low-level radio component, the unit price can be from $0,1 to $2 but you need a larger investment for the associated engineering.

Device technologies

POT – INDUS PHASES – Technologies

There are sensors available to get most of the environmental data. Each sensor capture one data. Sometime 2 or 3 when they are related.
Each sensor is a dedicated circuit with different characteristics in terms of precision, power consumption, price.
Sensors can be the main cause of end-device cost, this domain is also moving fast with edge computing and IA inside the sensors.

RISING IoT TECHNOLOGIES

EDGE COMPUTING AND NEURAL NETWORK (available)

More and more sensors includes neural networks. Optimized algorithm for IoT exists.

ULTRA LOW-COST (available)

Ability to make devices for a final price of $1 - $2. This is the enabler of IoT at scale with fleets of devices over 1M.

ULTRA LOW-POWER (to be)

Ability to make devices powered by the radiofrequency available locally. Consuming only picowatt, without chemistry.

Let’s make a short break

LEARNING AT THIS STEP

An IS team can manage an IoT POC

Thanks to the use of common technologies and existing products available on the market

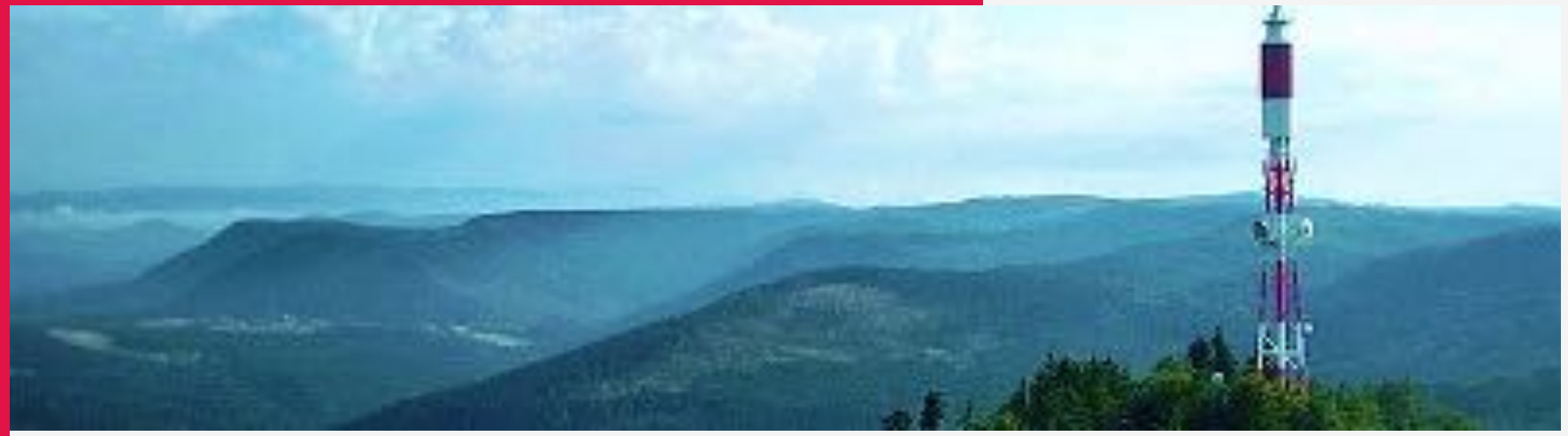
POT and INDUS require expertise

Something you can avoid by using product already existing on the market. Otherwise, build your team or find IoT contractors

IoT device is an optimized solution

IoT design is a good design when it perfectly fit with the expected behavior. It means it is dedicated to that specific use-case.

What are the main technologies in IoT communications ?



For human attached IoT

LOW POWER SHORT RANGE COMMUNICATION

Frequency: 2.4 -GHz
Tx power: 8dBm / 10mW
Pic current: 16,5mA
Coverage: 15m-30m
Throughput: 1Mb
Chip price: 1.5€ - 3.5€
Duty Cycle : 100%

Rq: v5 can go to 100mW / 300m outdoor

Bluetooth is equipping all modern smartphone and devices can use the Smartphone connections to reach Internet. That way the communication cost seems to be free for the consumers.
Bluetooth can also be used for Smart Home and Smart Building with long range version of thanks to meshed networks.
You need to know Bluetooth background communications with smartphone is complex to make working and diversity of smartphone is a big issue for Bluetooth IoT designs.

For home automation

ZigBee®

LOW POWER SHORT RANGE COMMUNICATION

Frequency: 2.4 -GHz
Tx power: 0dBm / 1mW
Pic current: 23 mA
Coverage: 100m / 30m
Throughput: 250KBps
Chip price: 5€
Duty Cycle : 100%

Rq: 100mW version exists for larger coverage

Zigbee and its competitor Z-Wave has been leader in smart home domain. They are not integrated into smartphone and need to have a Gateway to propagate the data to Internet and the central servers. This extra cost limit the application domains, mostly to smart home. Industrial domains also makes sense.
Zigbee also supports Meshed networks to extends the coverage.
Zigbee technical name : 802.15.4

For home & Industry big devices

HIGH-POWER SHORT-RANGE COMMUNICATION

Frequency: 2.4 –GHz (5GHz)
Tx power: 20dBm / 100mW
Pic current: 300 mA
Coverage: 30m
Throughput: 11Mbps (IoT)
Chip price: 1,5€
Duty Cycle : 100%

Rq: 802.11ah (HaLow) has been designed for IoT and operate sub-giga. But it is not really deployed yet.

WiFi have the advantage to be well deployed at Home and in the Industries & services. It have different negative points limiting its usage for IoT.

- The setup complexity
- The pic consumption over 100mA impacting the battery choice.
- The power consumption requiring large battery charge and short autonomy.
- WiFi requires a local gateway (access point), to communicate to Internet where the backend servers are.

For any low speed IoT context

LOW-POWER, WIDE-RANGE COMMUNICATION

Frequency: **868Mhz**
915MHz
2.4GHz
Tx power: **14dBm / 25mW**
20dBm / 100mW
Pic current: **30mA / 120mA**
Coverage: **500m - 10km**
Throughput: **5,6Kbps**
Chip price: **2€**
Duty Cycle: **1%-100%**

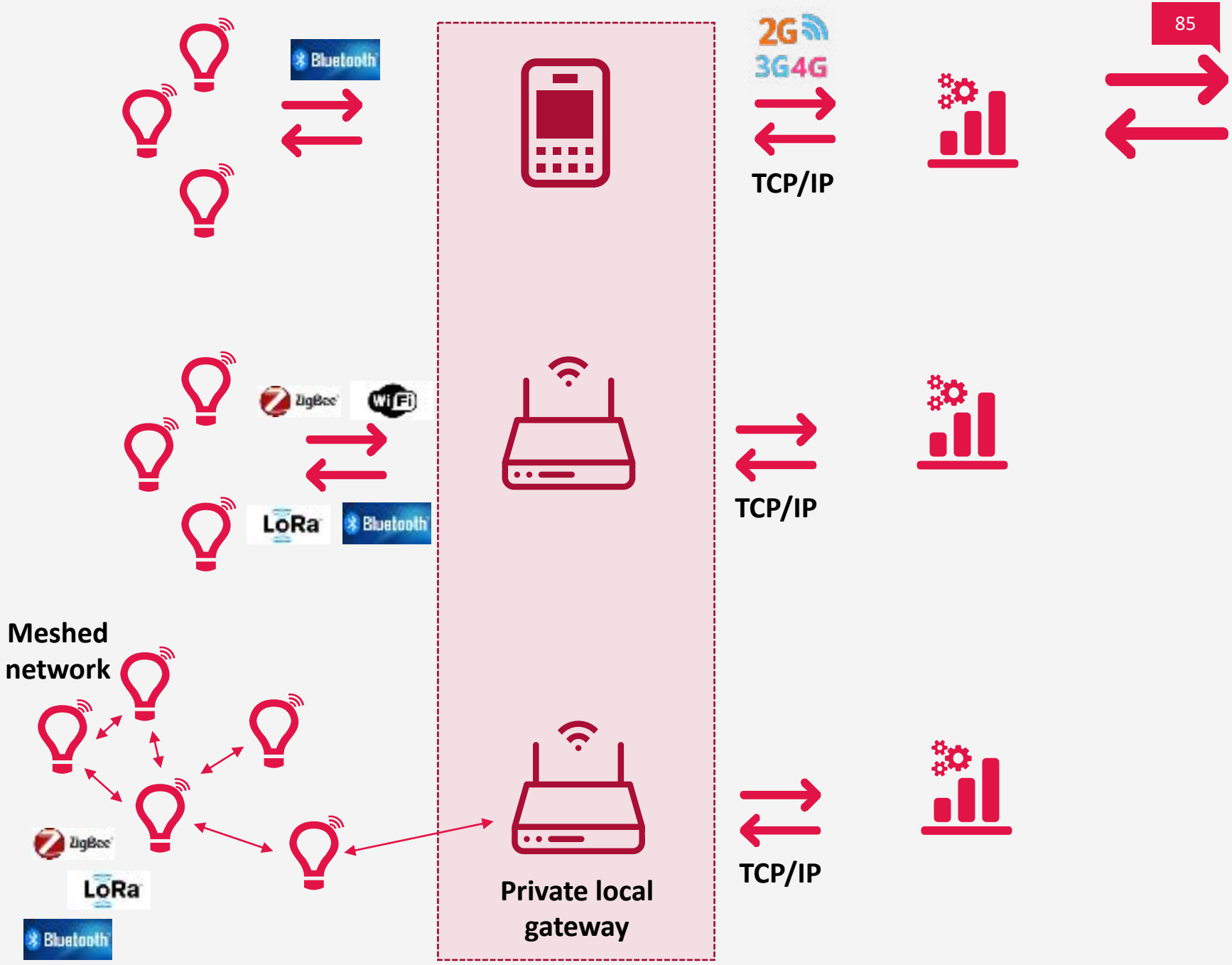
LoRa is a point to point radio communication solution allowing wide range coverage. Indoor application, device to device are offering around 500m coverage when outdoor usage will reach 10km to 15km. LoRa needs to be connected to a gateway to access Internet and backend service.

LoRa is used in different smart home solutions, speed, bandwidth, power consumption can be adapted regarding the use-cases.
We see some meshed implementation of LoRa rising, allowing to cover cities with crowed sourced network.

Point to point IoT communications architectures

All the previously seen technologies are not TCP/IP based and able to communicate on Internet.

So we have some common architecture related to these technologies where a locally deployed gateway allow to translate the communications to TCP/IP to interact with the solution platform.



For autonomous short autonomy IoT

GSM UMTS LTE

HIGH POWER
HIGH SPEED
LONG RANGE
COMMUNICATION

- Frequency: **700MHz – 3.7GHz**
- Tx power:
  - 2G: **33dBm / 2W**
  - 4G: **43dBm / 20W**
- 3G/4G EU: **24dBm / 0.25W**
- Pic current: **250mA-2,5A**
- Coverage: **5km – 100km**
- Throughput: **1Gb**
- Chip price: **3€ - 20€**
- Duty Cycle: **100%**

Technologies from 3GPP consortium are common when you have externally powered device or the ability to recharge the device on regular basis.
This technology allows large amount of data transfer with a global worldwide coverage. There is no usage restriction basically.

The most complex part is to manage the subscription and the SIM or eSIM card with NVNO, Multi-operators, dynamic subscription…
For IoT design, battery cost and module cost will impact the business model with limited value creation.

Communication technologies

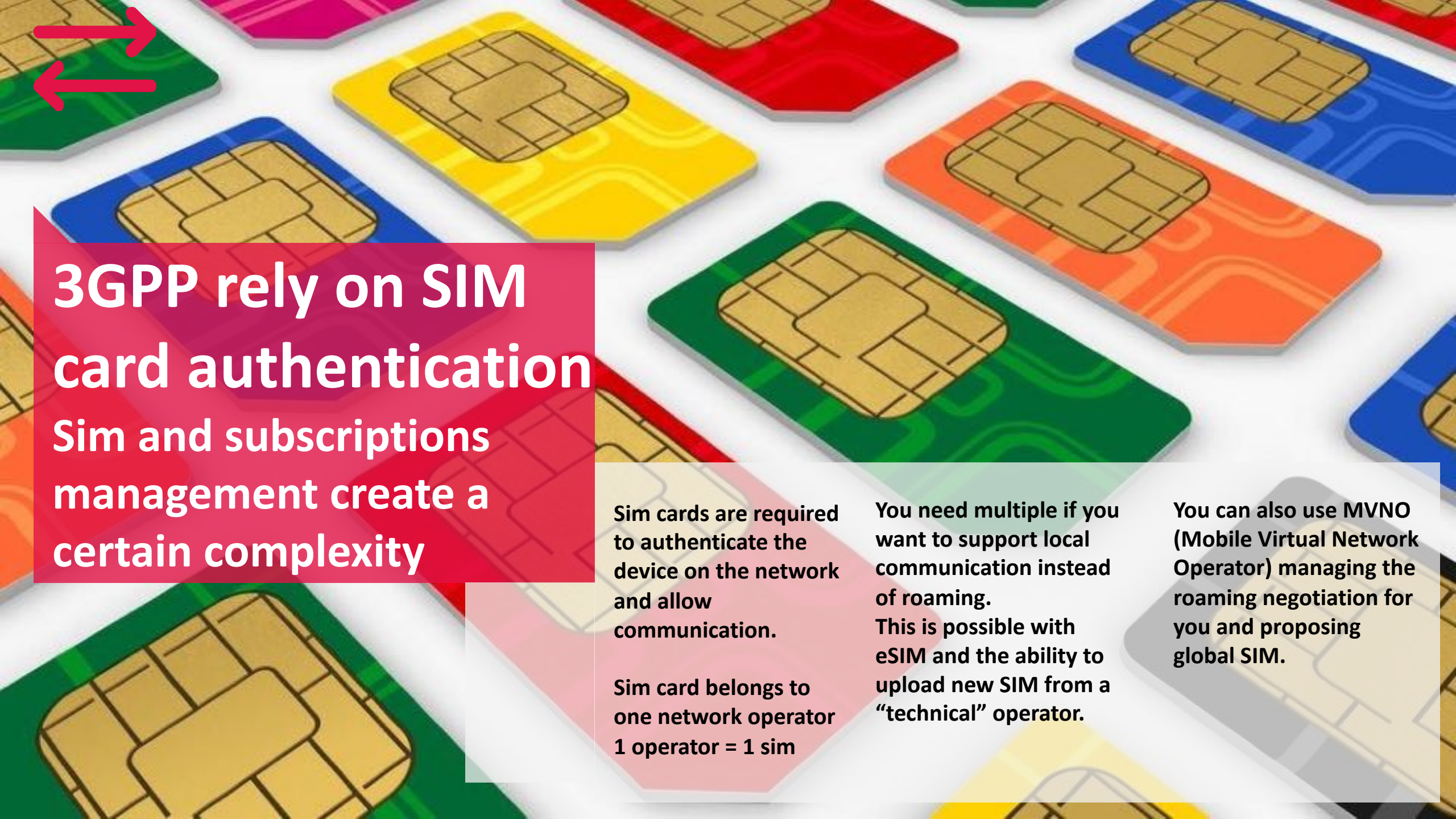
For autonomous static IoT with IP

“LOW” POWER
HIGH SPEED
LONG RANGE
COMMUNICATION

Frequency: **700MHz – 2.6GHz**
Tx power: **23dBm / 0.20W**
Pic current: **250mA**
Coverage: **5km**
Throughput: **4Mb**
Chip price: **10€**
Duty Cycle : **100%**

CAT-M0 / CAT-M1 / CAT-M2

LTE-M is a low power solution for LTE technologies. It has been added in the 4G and it will be improved in the coming 5G.
Basically it allows a device to deep-sleep for a long period of time, then resume quickly on the network for short communications. It works well until the device move out from the network cell.
LTE-M can be deployed where 4G is, not all country currently support it but it the easier to find worldwide.
Fallback to 4G/3G is recommended. Expected energy savings are uncertain.



3GPP rely on SIM card authentication

Sim and subscriptions management create a certain complexity

Sim cards are required to authenticate the device on the network and allow communication.

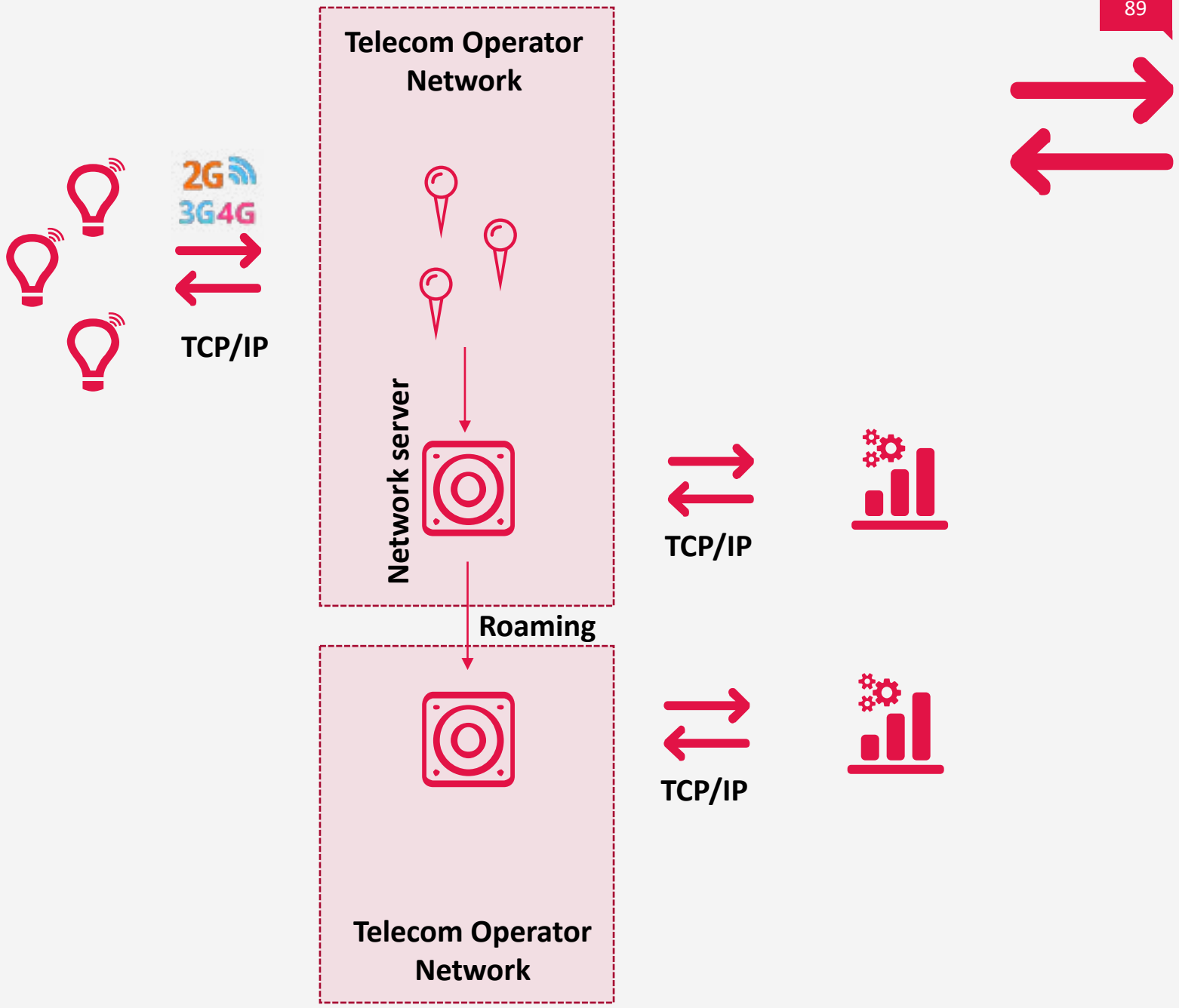
Sim card belongs to one network operator
1 operator = 1 sim

You need multiple if you want to support local communication instead of roaming.
This is possible with eSIM and the ability to upload new SIM from a “technical” operator.

You can also use MVNO (Mobile Virtual Network Operator) managing the roaming negotiation for you and proposing global SIM.

3GPP classical solutions are IP based

The device can directly communicate over TCP/IP.
IoT subscription will sometime require a public IP attribution for a direct communication with the device.
These technical solution also simplify device-to-device communication and massive downlink.



LPWAN - 3GPP Low Power

CAT-NB1 / CAT-NB2

LOW POWER
MEDIUM SPEED
LONG RANGE
COMMUNICATION

Frequency: **800MHz – 1.8GHz**
Tx power: **23dBm / 0.20W**
Pic current: **250mA**
Coverage: **10km**
Throughput: **160Kb**
Chip price: **5€**
Duty Cycle : **100%**

NB-IoT is a low power solution for LTE technologies. It has been added in the 4G and it will be improved in the coming 5G.
NB-IoT is different than LTE technologies and simplify it. This allows to have simplified hardware with a lower cost and lower power consumption. The number of NB-IoT networks, worldwide, is still low but this is really promising. The main issue is the roaming between operators for devices moving out of the operator coverage.
Coverage is directly related to 4G coverage. A sim is needed.

Communication technologies

LPWAN – For deep IoT

LOW POWER
LOW SPEED
LONG RANGE
SECURED
COMMUNICATION

Frequency: **169MHz**
Tx power: **27dBm / 0.5W**
Pic current: **500mA**
Coverage: **50km**
Throughput: **2.4-6.4Kbps**
Chip price: **5€**
Duty Cycle : **10%**

Last technology rising on the LPWAN area, Wize has been pushed by Suez and GRDF to support the water and gaz counters telemetry. For this reason a particular attention has been made on communication encryption. The 169MHz choice made this network really fitting with deep indoor communication. The coverage is limited to France, Spain, Portugal, Italie, UK, Moroco, Algeria but the real coverage out of main cities is currently unclear.
The technology is new, the ecosystem still limited, this could be promizing for smart city & smart building.

LPWAN – Private IoT networks

LOW POWER
LOW SPEED
LONG RANGE
COMMUNICATION

Frequency: **868Mhz**
915MHz
2.4GHz
Tx power: **14dBm / 25mW**
20dBm / 100mW
Pic current: **30mA / 120mA**
Coverage: **10km**
Throughput: **5,6Kbps**
Chip price: **5€**
Duty Cycle : **1%**

LoRaWAN is a network implementation of LoRa technology. It can be used with public and private networks. Public(nation wide) deployments are really limited over the world and the main use concerns private deployment. The network cost is low (gateways starts at 70€). Some crowdsourced networks like TTN or Helium also complete the public offering. France have 2 LoRaWan public networks with nationwide coverage. This is an exception.

It is the only LPWAN you can use without a subscription business mode. The complex software stack requires a strong MCU.

Communication technologies

LPWAN – Global worldwide network

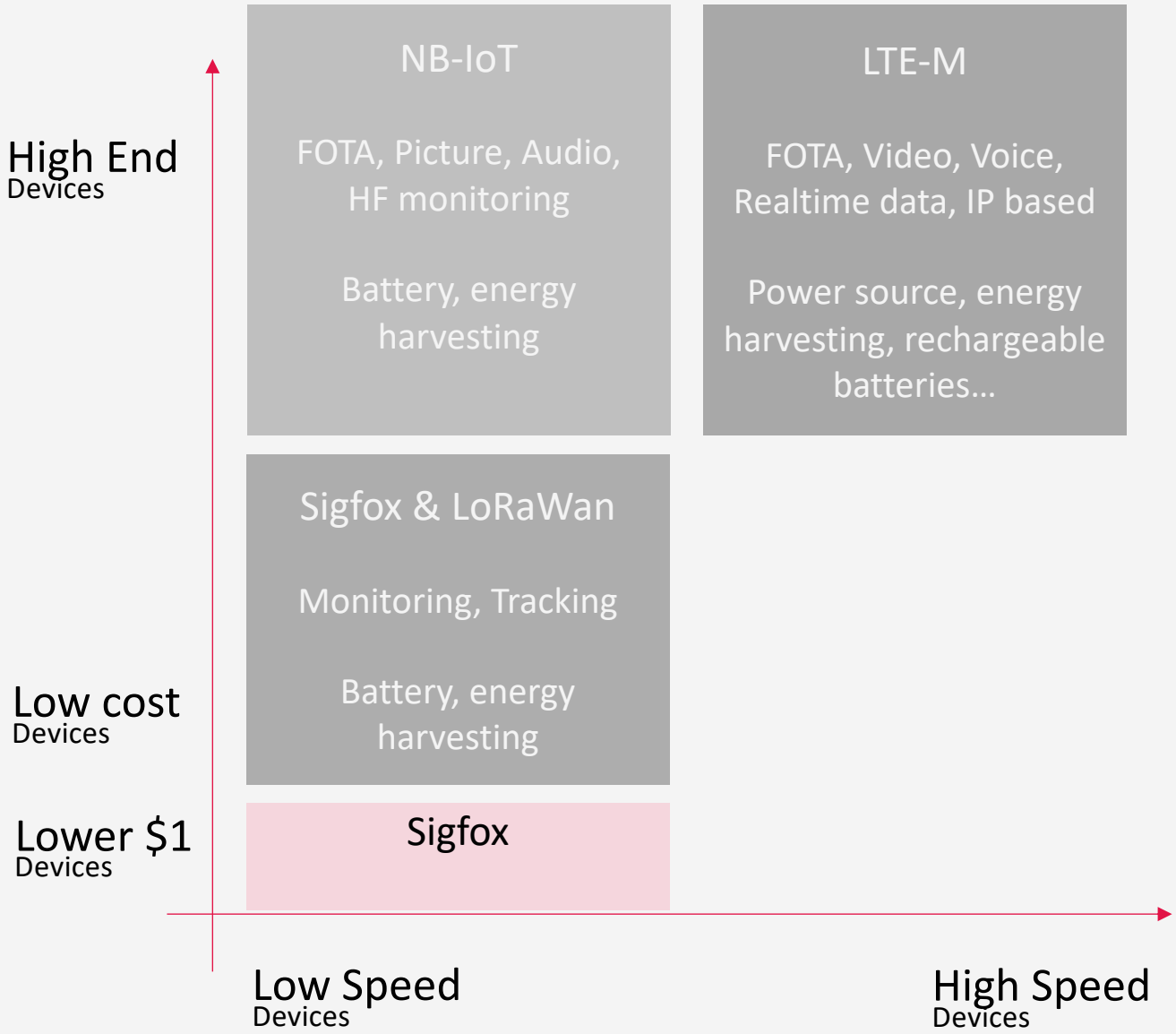
LOW POWER
LOW SPEED
LONG RANGE
COMMUNICATION

Frequency: **868Mhz**
915MHz
Tx power: **14dBm / 25mW**
20dBm / 100mW
Pic current: **30mA / 120mA**
Coverage: **40km**
Throughput: **100/600bps**
Chip price: **0.2€ - 4€**
Duty Cycle : **1%**

Sigfox is a radio technology (UNB) and a public network operator operating a SDR radio network.
The asymmetry of the technology allows and long-range performance for simple transceiver.
This is the first technology to enable the Ultra Low Cost IoT (finished devices under $1)
The key differentiator of Sigfox is being the only one worldwide network operator. Sigfox is a single network with a single network server.
Sigfox is a French company.

Technologies Are NOT in competition

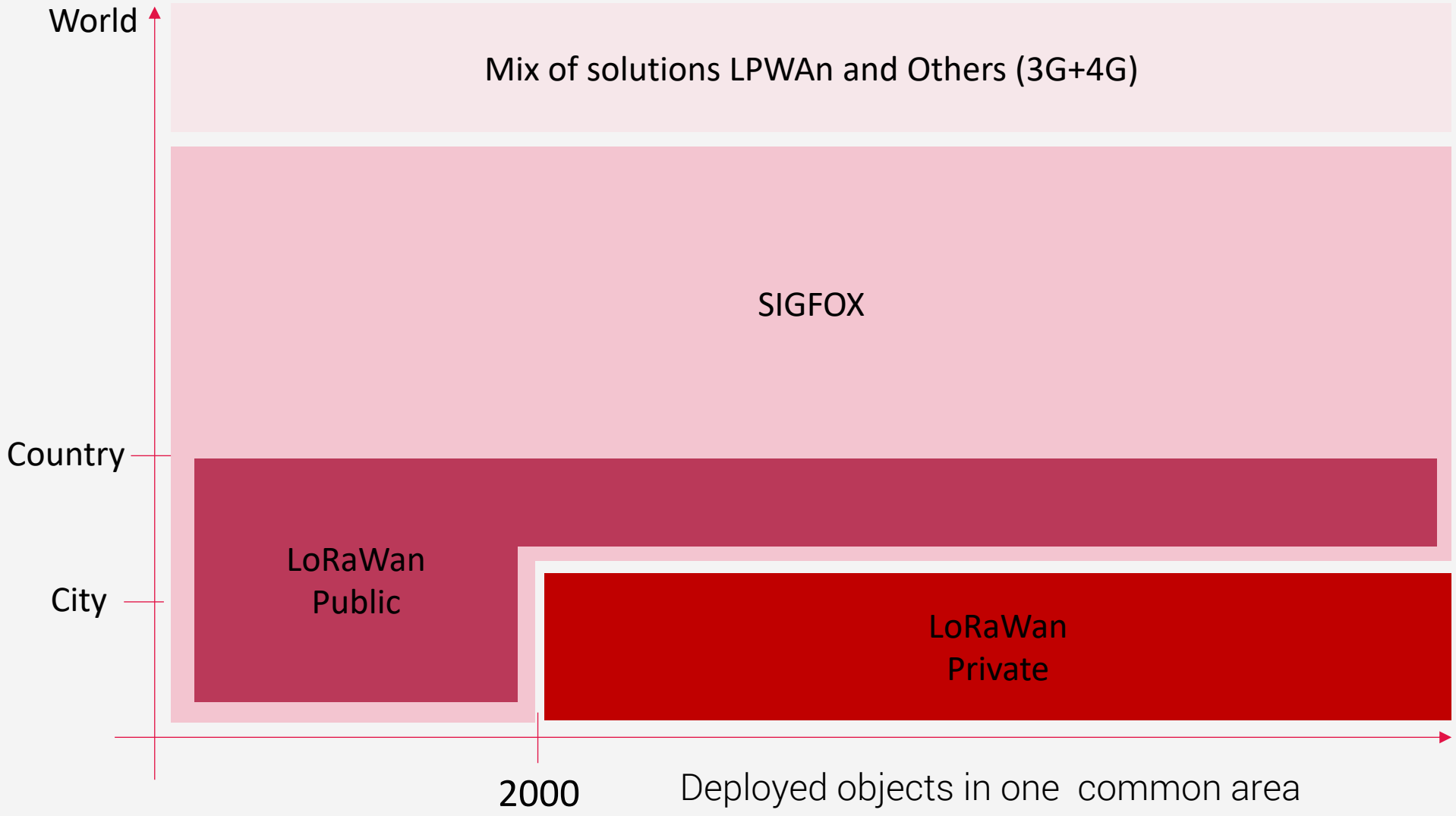
They are addressing different use-case, with different total cost approach related to **speed** and **power consumption**.



Sigfox LoRaWan

Low-cost devices

More than the technical difference to serve a specific use-case we can generally tweek, the choice is related to the targeted **deployment scope** and **model**.



NB-IoT, Wize, LoRaWAN, SIGFOX are the key player of the IoT revolution

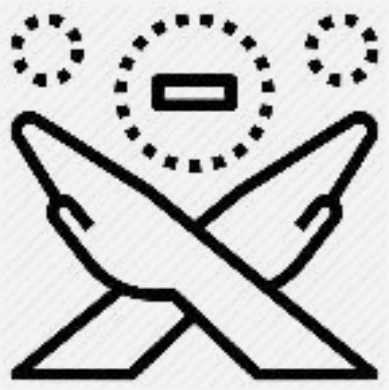
They are the

LPWAn

Low-Power
Wide Area
Networks

LPWAN are the revolution solving this dilemma:

Low-Power Transmission



Long-Range (wide area)

=

Long autonomy
(in years)

=

Low cost networks
(1 country deployed costs the price of 1 big city with 4G)

Low cost subscriptions

LPWAN are enabling the “IoT at scale”

IoT at scale is the ability to deploy and manage large fleets of devices, over millions with a viable business model

To connect all kind of existing things, you need to:

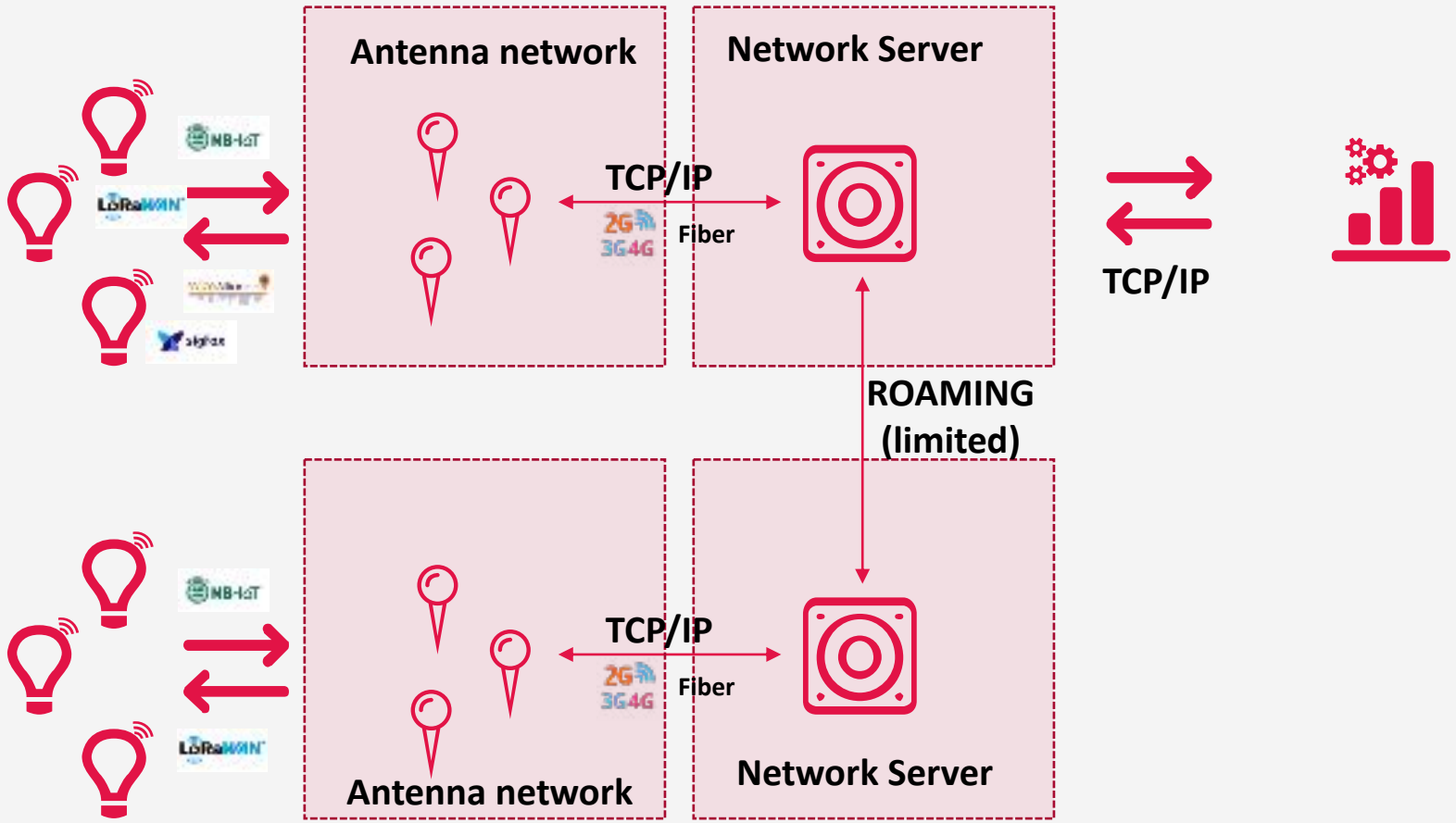
- **Break the device cost**
- **Break the communication costs**
- **Allow years of autonomy w/o maintenance**
- **Eliminate user setup**
- **Reduce the battery size**
- **Break boundaries**
- **Cover the world**

LPWAN have a common architecture

The devices messages are captured by multiple antennas around.

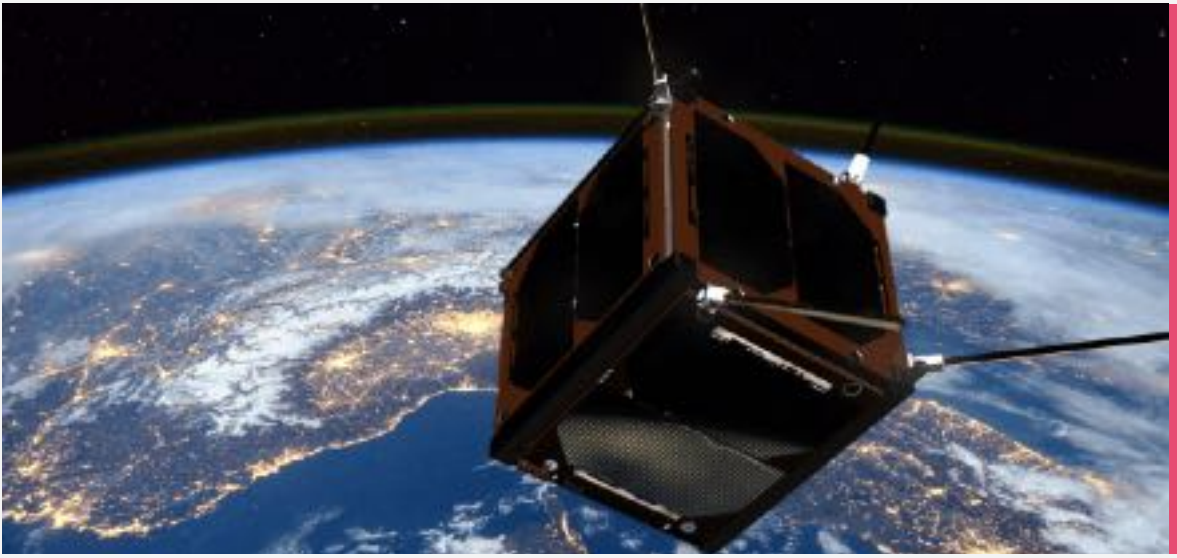
The antennas forward the messages to a network server owned by the network operator (private or public)

Then the network server transfers the payload to the custom backend, eventually, roam it to another network server.



IoT everywhere with satellites

(Argos)



GLOBAL COVERAGE
LOW POWER
COMMUNICATION

kinéis

Lacuna space

sigfox

(LoRaWan)

Multiple IoT operators are looking to the sky to provide a global coverage, particularly on ocean and desertic zones. With a fleet of 15-20 satellites you can cover the world with a communication capability every 10 - 15 minutes for the devices. For Sigfox the objective is to propose device able to communicate with satellite and terrestrial network, all in one. Lacuna and Kineis are satellite only.
The challenge is the synchronization with sats.
Compared to Facebook, Google, Musk project requiring advanced transceiver, the IoT solution are really simple and use simple, not motorized, antennas.

Let’s make a short break

LEARNING AT THIS STEP

There is a large range of technologies

They are not really in competition as they are addressing different type of IoT and different use-cases.

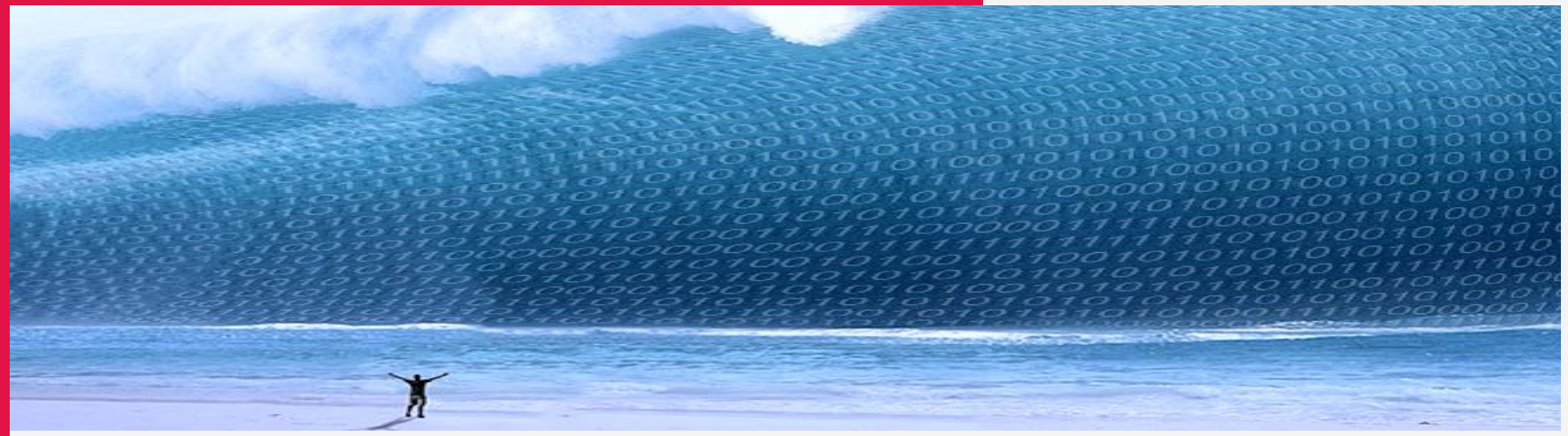
The architecture depends on the technology

The technology determines the architecture and the running costs

LPWAn are the IoT revolution

LPWAn are key enabler for Low Power, Low Cost Iot allowing IoT at scale = IoT in all the things

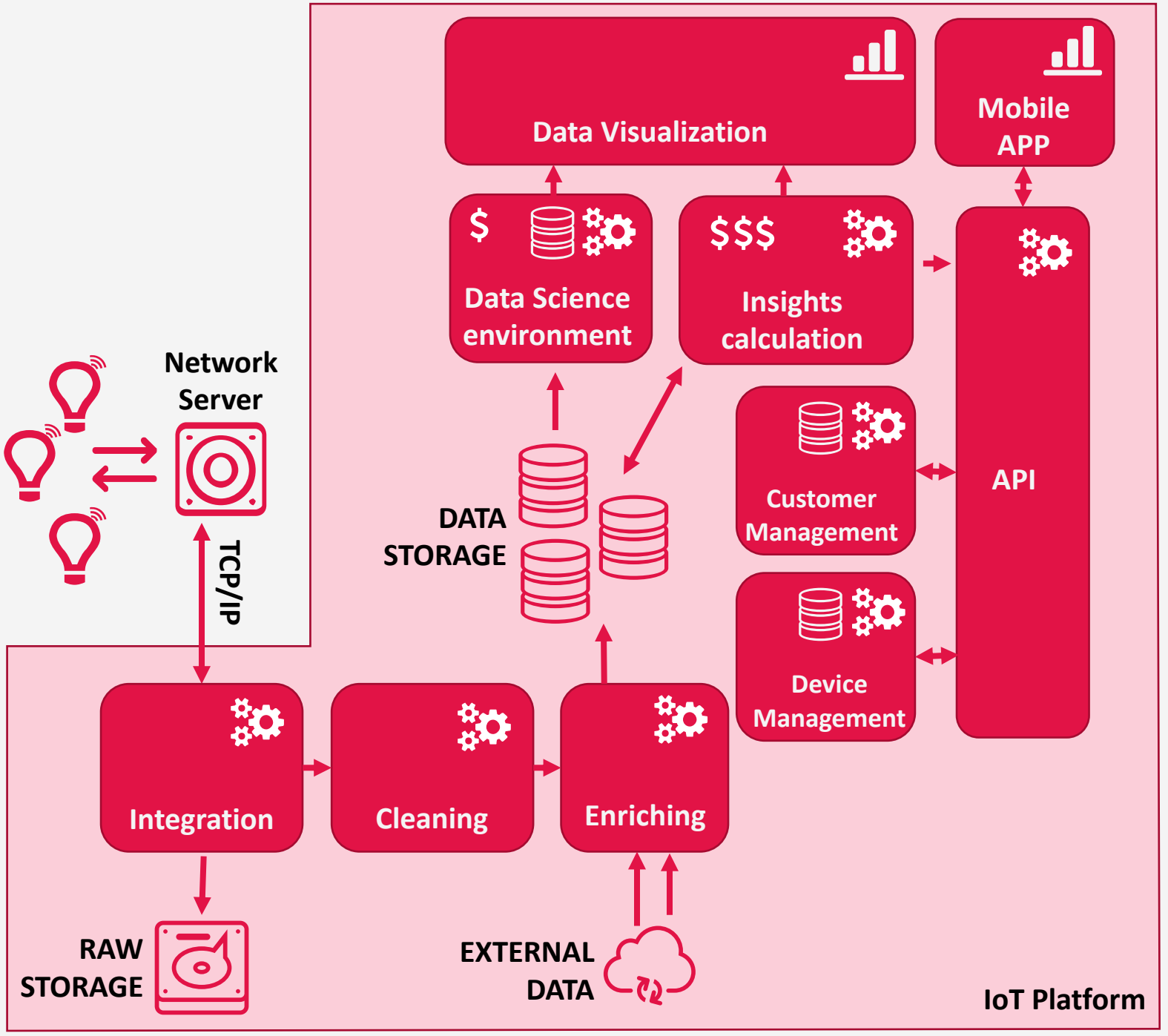
How to process the IoT Data ? Common architecture, technologies…



Main components of an IoT platform

An IoT platform is a complex IT architecture where some of the components are highly critical like the “Integration” layer

All the processing layers must be ready for Big Data and scalable.



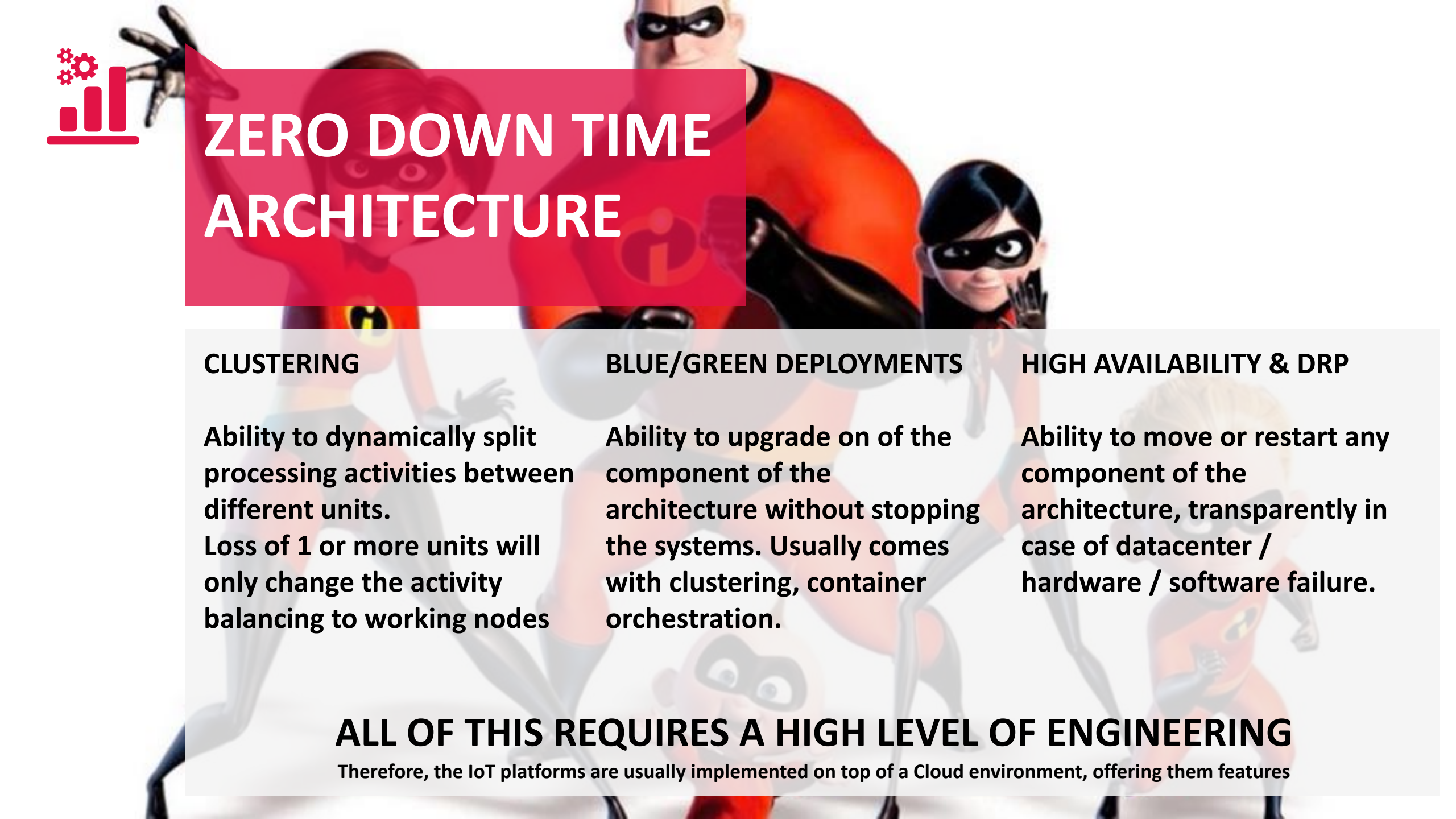
CLOUD PLATFORMS AS A REQUIREMENT

The integration layer can’t stop, at any time, because IoT will never pause the transmissions and large Things fleets will always transmit data (by opposition to classical Human activities)

This requires 0 down time capabilities

The power of IoT is to consolidate and process the full history of data making the processing bigger and bigger even with a stable fleet of devices. The Thing’s fleet is also subject to scale.

This requires infinite scalability capabilities



ZERO DOWN TIME ARCHITECTURE

CLUSTERING

Ability to dynamically split processing activities between different units.
Loss of 1 or more units will only change the activity balancing to working nodes

BLUE/GREEN DEPLOYMENTS

Ability to upgrade on of the component of the architecture without stopping the systems. Usually comes with clustering, container orchestration.

HIGH AVAILABILITY & DRP

Ability to move or restart any component of the architecture, transparently in case of datacenter / hardware / software failure.

ALL OF THIS REQUIRES A HIGH LEVEL OF ENGINEERING

Therefore, the IoT platforms are usually implemented on top of a Cloud environment, offering them features

INFINITE SCALLING CAPABILITIES

CLUSTERING

Ability to dynamically add new processing node to a computing engine.
Ability to support linear processing time in regard of the number of nodes.

COMPUTING RESOURCE ON DEMAND

Ability to scale the processing engine on demand, to extends the capability in a large order of magnitude progressively or just for a couple of hours.

PRICE LINEARITY

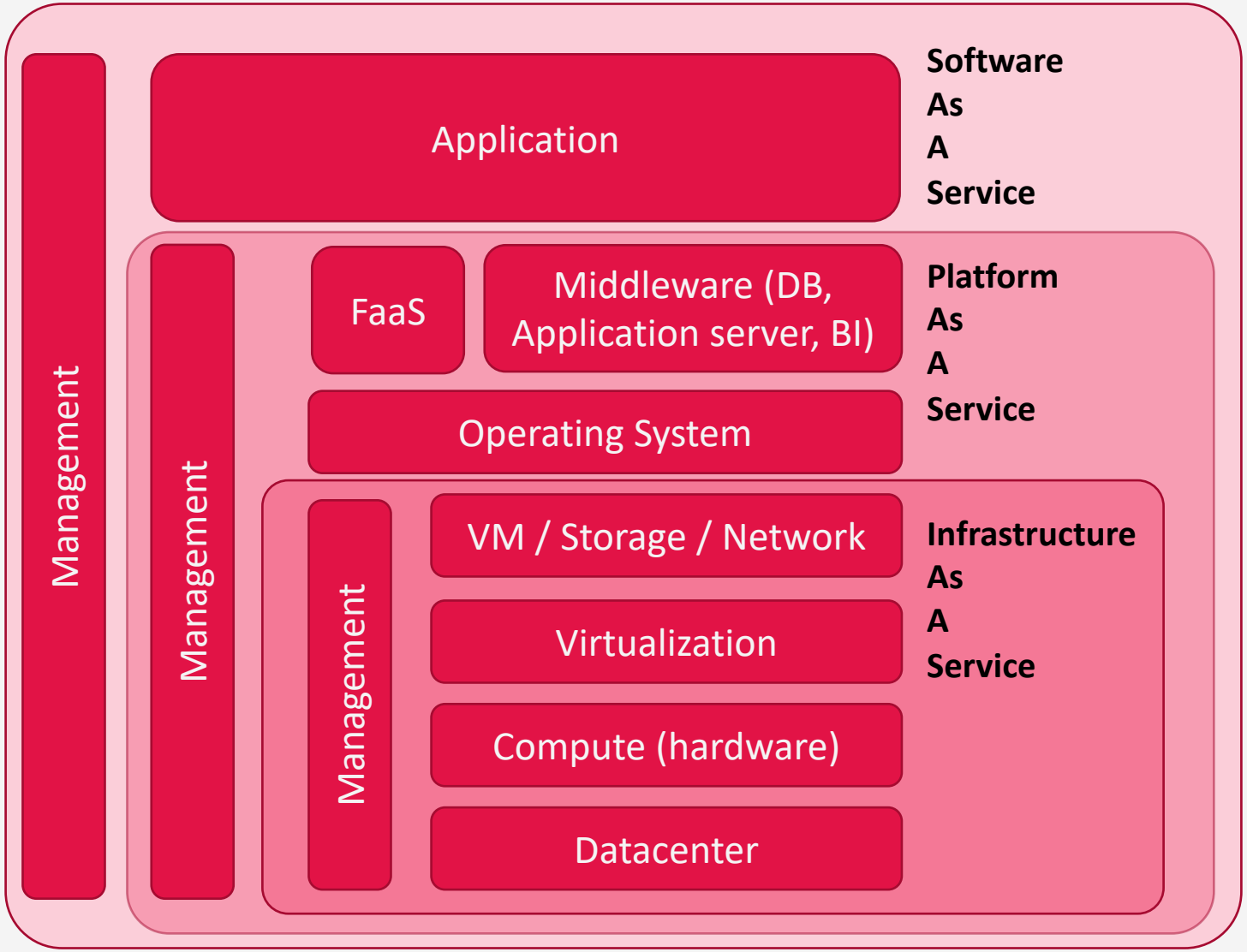
Ability to scale the architecture and process capability with a linear progression of the costs, whatever the scale.

ALL OF THIS REQUIRES A HIGH LEVEL OF ENGINEERING

Therefore, the IoT platforms are usually implemented on top of a Cloud environment, offering them features

Main cloud concepts

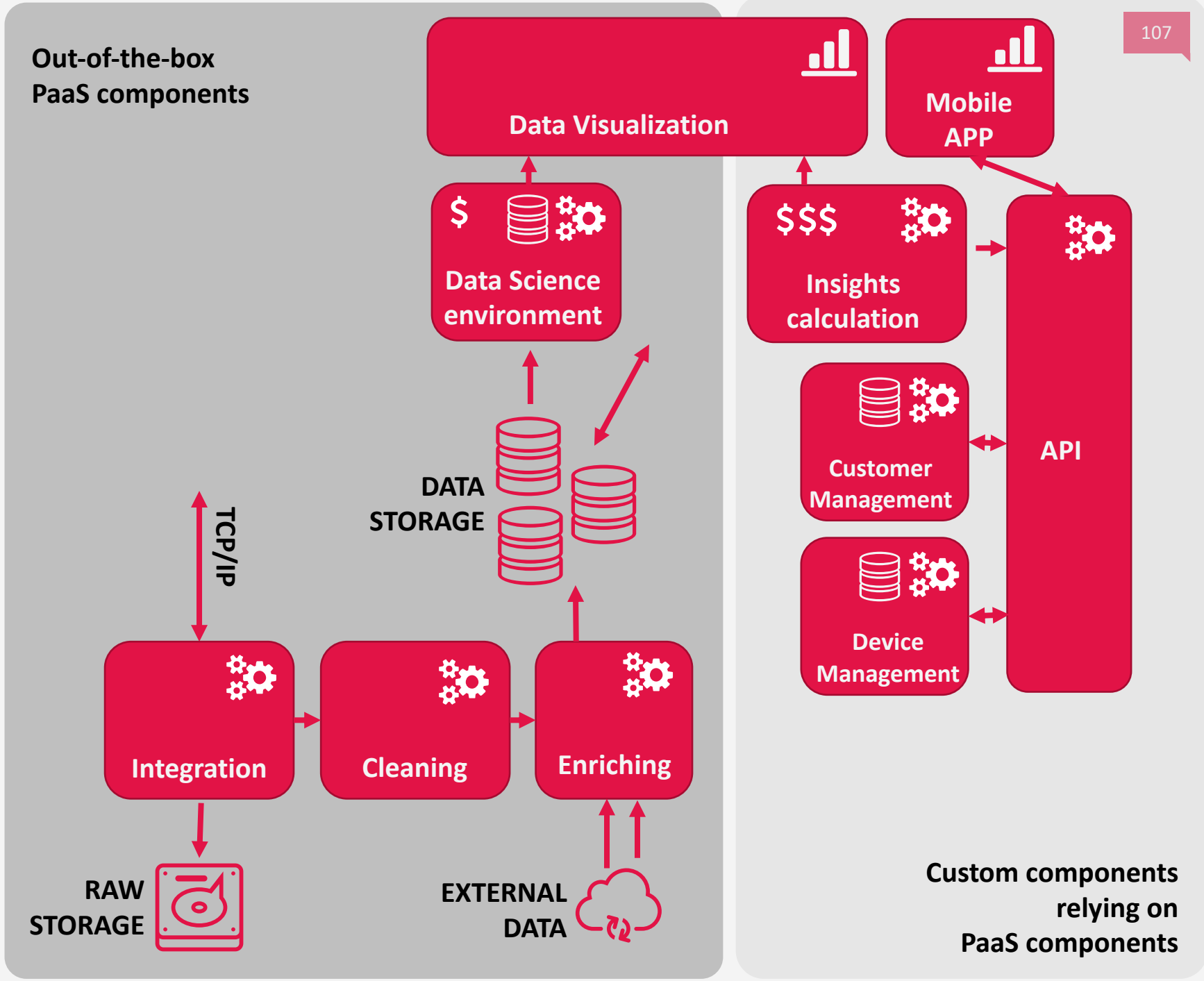
Using a cloud environment for you IoT platform will reduce your need of expertise on the critical infra components.
Cloud is providing a certain level of management and associated SLA depending on the level you select.



Use of Cloud for IoT platforms

Most of the components will take a benefit of a PaaS approach.

Integration layer to the data visualization are Out-of-the-box existing PaaS pattern ready to be deployed in a single click in most of the Cloud providers.



Data is a precious assets which implies responsibility

PERSONAL DATA

B2C IoT requires to register user and these data are personal data.
Furthermore, IoT is capturing data, personal data like for a geolocation system. Heath data when recording activities, heart rate…

ANONYMIZATION

To be reused in multiple secondary business, the anonymization of the data is a key point. This is also a good way to keep the personal and health data for a long time. Personal data can't be.

ENCRYPTION

To ensure data protection, encryption is a state-of-the-art solution.
It is also a protection against data leak: your IoT data are an asset, the value of this assets comes from scarcity - don't be your own competitor.

Let’s make a short break

LEARNING AT THIS STEP

Processing IoT is an infrastructure challenge

Due to the criticality of the data integration

The Cloud providers can be the solution solution

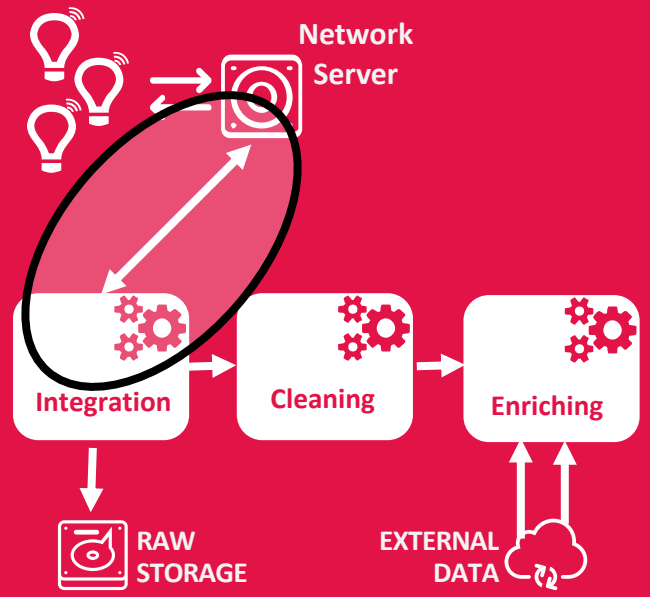
Complex infrastructure are easier when managed by experts

Iot Data are sensitives assets you need to protect

So you can focus on your data protection which have a larger value for your business

Data Integration

This component is highly critical and can be implemented in different ways



Integration

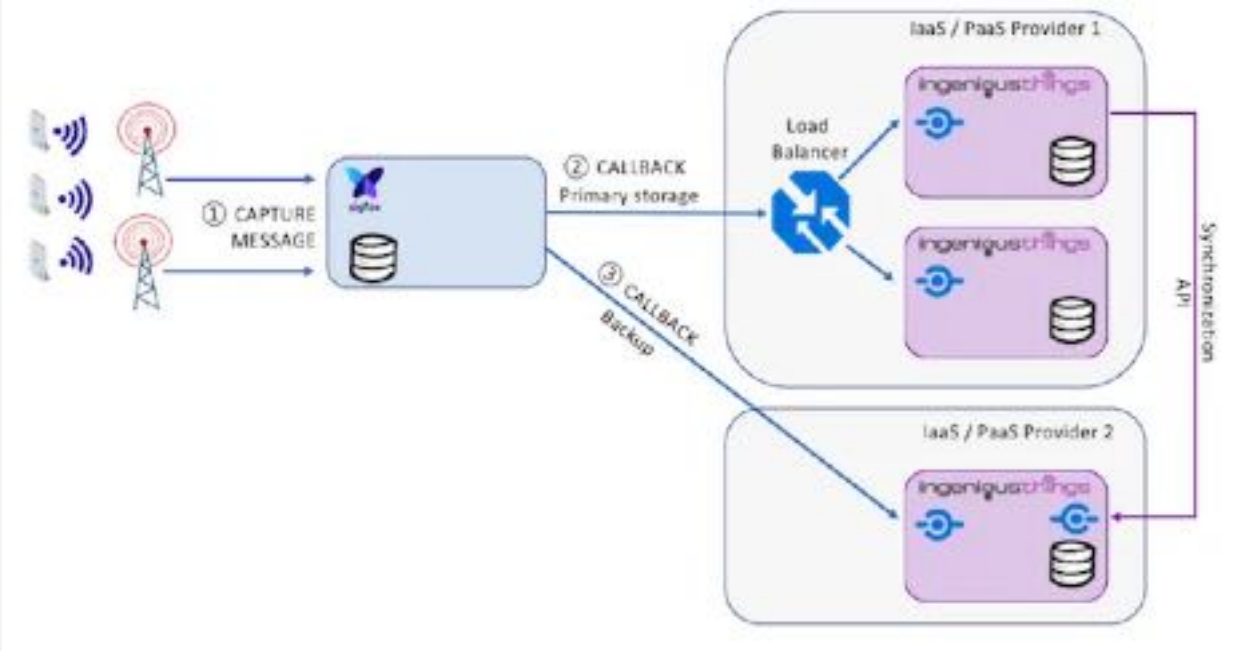
SOLUTION 1

PUSH - HTTP Integration (Callback or Webhooks)

The Network server calls an API on the Integration Layer on every message received / on every seconds when messages have been received.

Common technical solutions:

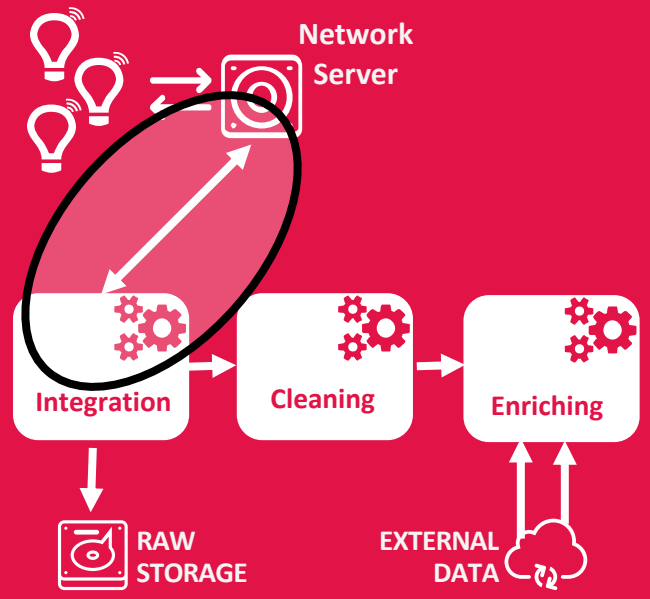
- API Cluster with backup or multiple sites.
- FaaS (Function as a service)



This solution is fully synchronous . As this kind of solution presenting a risk of data loss, there is a backup solution with an asynchronous synchronization mechanism.

Data Integration

This component is highly critical and can be implemented in different ways



Integration

SOLUTION 2
PUSH – Message Queue based integration

The Network server push messages over a broker managing message queues. That way, the communication is asynchronous between the Network server and the Data integration layer.

Common technical solutions:

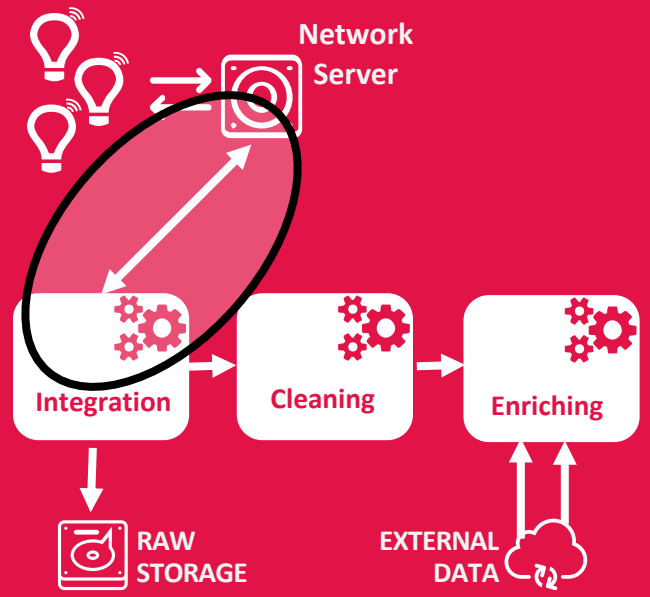
- Use of MQTT (most frequent with IoT)

  MQTT is a lightweight queuing protocol over TCP managing quality of service. It works well as a cluster.

  TCP/IP ready devices can directly implement MQTT communication to report data. This is working will well with low quality networks (like cellular networks).

Data Integration

This component is highly critical and can be implemented in different ways



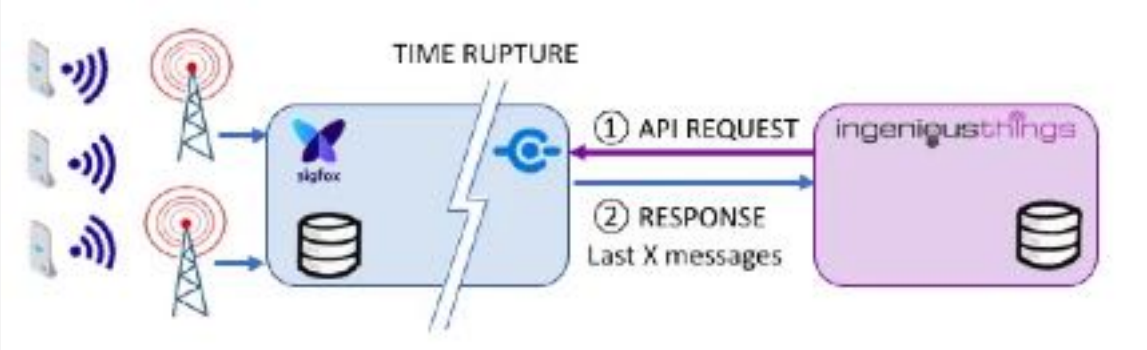
Integration

SOLUTION 4
PULL – API CALL ON THE NETWORK SERVER

The application request status of device and extract data from the Network server with API calls. That way the application integration layer is not critical.

This solution is not really recommended until you have large fleets because it creates a time rupture between device's message reception and message processing. So you are not real time anymore.

When your device fleets becomes large and you have message on every seconds, this integration way makes sense to preserve the application resources and reduce the criticality of the integration layer.



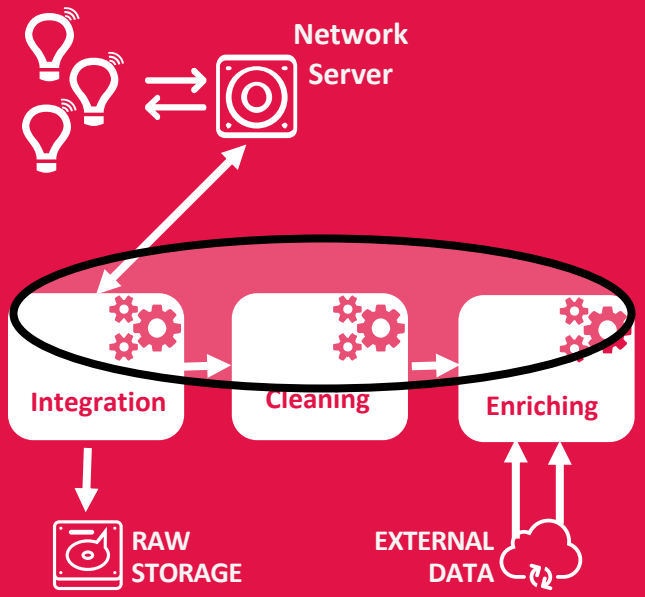
Integration

CONCLUSION INTEGRATION LAYER

The way the integration layer is implemented depends on the technical solution offered by the Network Server.
It also depends on the fleet size and the frequency of the messages you need to integrated.

REAL-TIME, EVENT PROCESSING

The integrated data is then process, clean, enriched in real time, because users want to see it immediately.

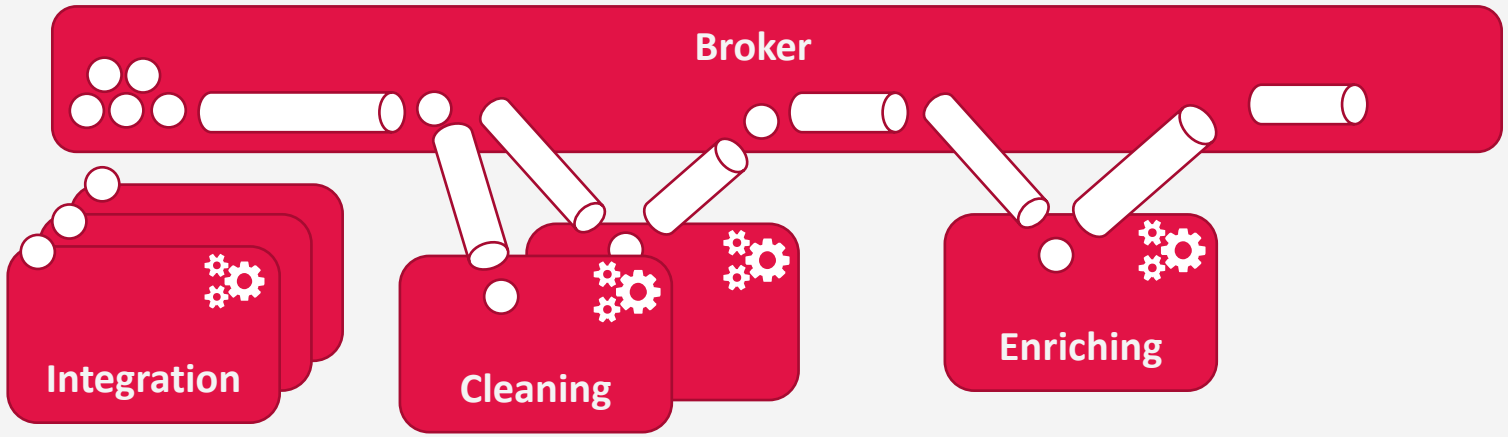


Integration
Cleaning
Enriching

Solution 1 - Message Queuing

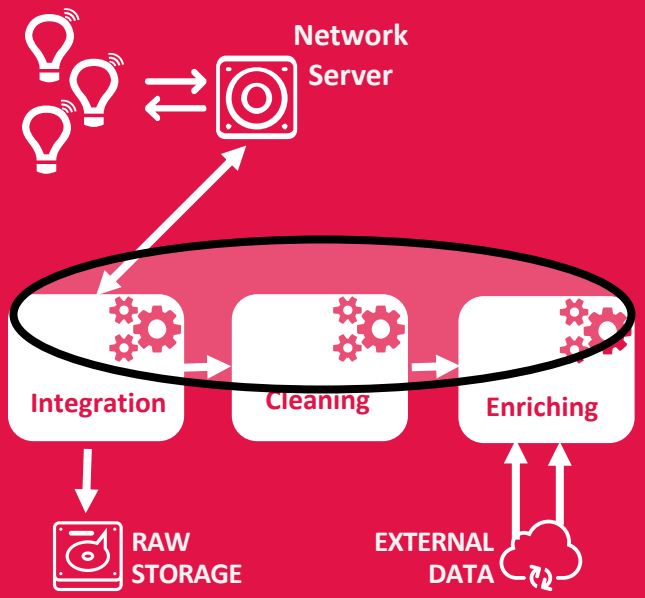
One of the problem to solve is the fluctuation of the workload depending on the sensor communications. This workload is composed by a series of messages to process the same way, individually.
One of the pattern is to transform each of the sensor communication in a message send to a Queue. This queue will be consumed and process by the next layer, asynchronously. Scalability is easy to manage as concurrency.

The second problem to solve is the ability to reprocess the whole history because you changed some of the intermediate processing. For the same reasons, this solution is also efficient.



REAL-TIME, EVENT PROCESSING

The integrated data is then process, clean, enriched in real time, because users want to see it immediately.

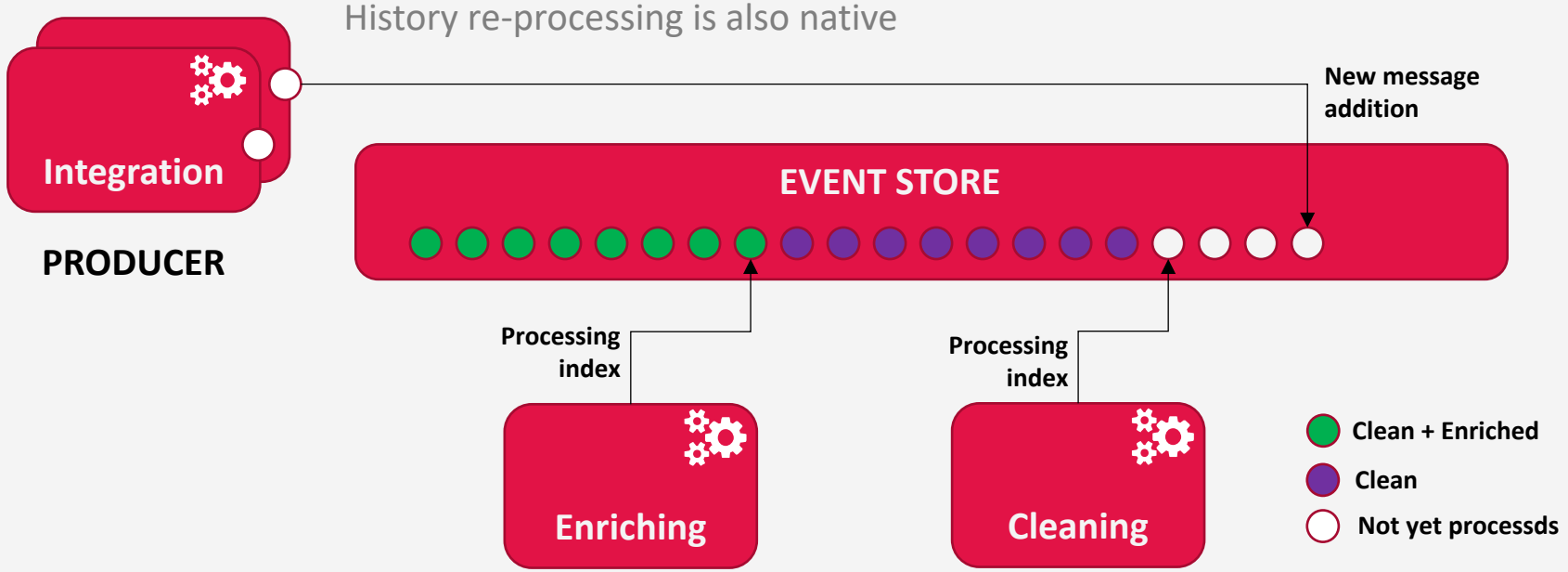


Integration
Cleaning
Enriching

Solution 2 – EVENT SOURCING

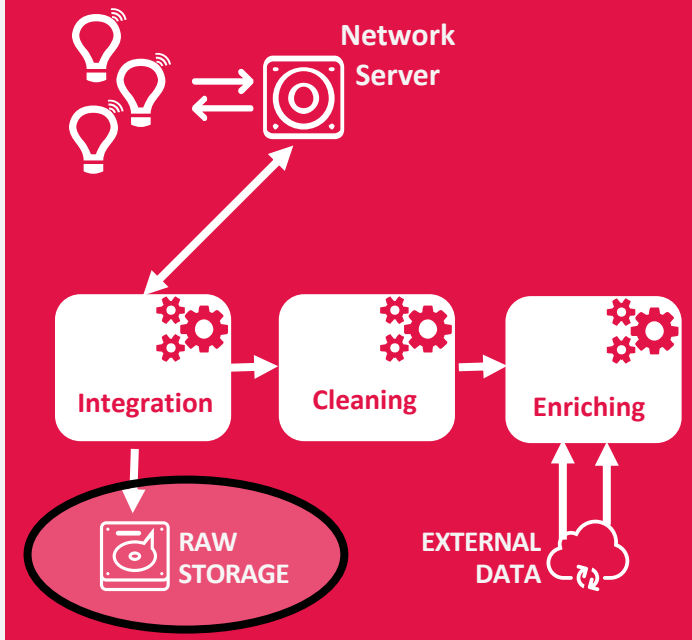
Event sourcing is working a similar way with a major difference. In a Message queue architecture, the message is going in and out but not stored. Updating the broker or scaling the broker itself can be a problem. In production the broker can also become saturated if some consumer are dead or undersized to process the messages. Dynamically changing the process tree can also be an issue.

Event sourcing (product like Kafka) is solving this issue with a more scalable architecture. The integrated producer / consumer approach, working directly on the data flow is also very efficient.
History re-processing is also native



STORE RAW DATA FROM SENSORS

Because once refined you lost information and future value.



RAW STORAGE

STORE THE RAW DATA

DATA is an asset, every time to modify the raw data, you loose a part of the information. Even if at a certain time you think not to do it, later you may discover you were.

Furthermore, it is recommended to keep your processing chain to be able to recompute everything from the first day. It means, the computation data source will be the RAW DATA.

The reason is: more data you have, more insight you create. Most insight will learn from the past and create value even in the past.

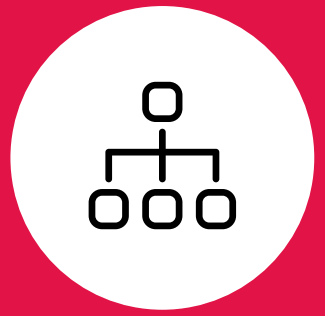
This RAW DATA volume, over the years will take more and more space and some specific technologies could be required. Some technology are use for this.

- Kafka: scalable event store
- Hadoop: scalable file storage
- Mongo DB: scalable NoSQL Databases

The advantages of NoSql database compared to standard SQL database is the native clustering mode but also the ability to mix different sort of message payload in a common repository. Sensors messages will evolve with versions over time, you need to anticipate this.

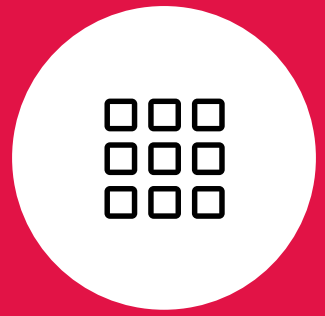
Let’s make a short break

LEARNING AT THIS STEP



Many patterns exist to support the data integration

You need to design the solution based on your target volume of data and fleet size



All the technologies are cluster and scalable

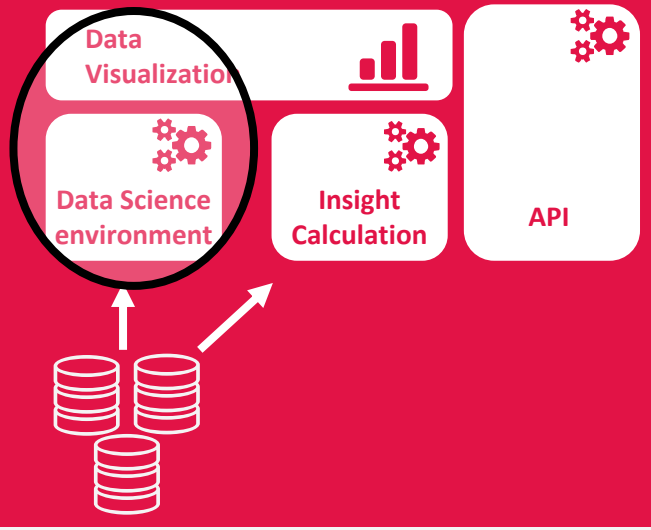
That’s a key factor of success for a critical component of the solution

Be prepared to reprocess everything

Your future business will require data processing you can’t imagine today.

Extract value from DATA

Data Science analyze data and propose solution for Insights calculation.
Classical BI allow to display results.



Data Science environment

Laboratory for your data

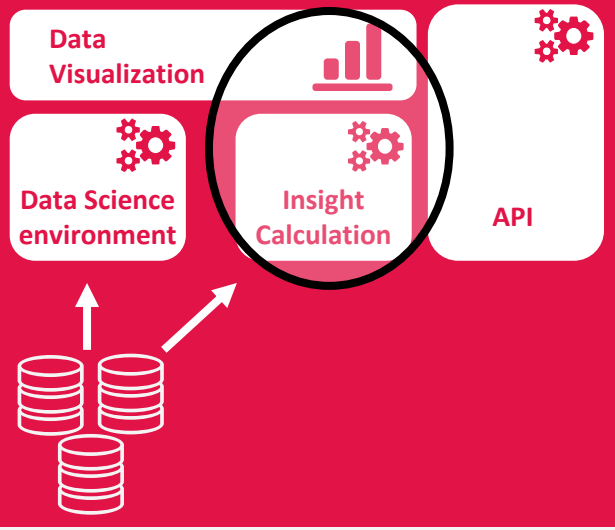
Data Science experiment the data to create added value insight, performant neuronal networks or statistical studies.
The data science work is growing with the size of the dataset and the number of market your solution can address.

The classical tools for data scientists are:

- R or Python development environment
- Parquet like columnar storage format
- BI reporting environment to create dashboard
- Neural networks execution platform (GPU…)
- Large access to the raw data, enriched data and external data.

Extract value from DATA

Data Science analyze data and propose solution for Insights calculation.
Classical BI allow to display results.



Insight calculation

Your product is here

An IoT solution should only distribute Insights and not the Raw data:

- Because its role is to create a proper value
- Because giving raw data makes its value going down to 0.

An Insight is basically the industrialization of the data-scientist work. It must be computed in real time when new data have been received.

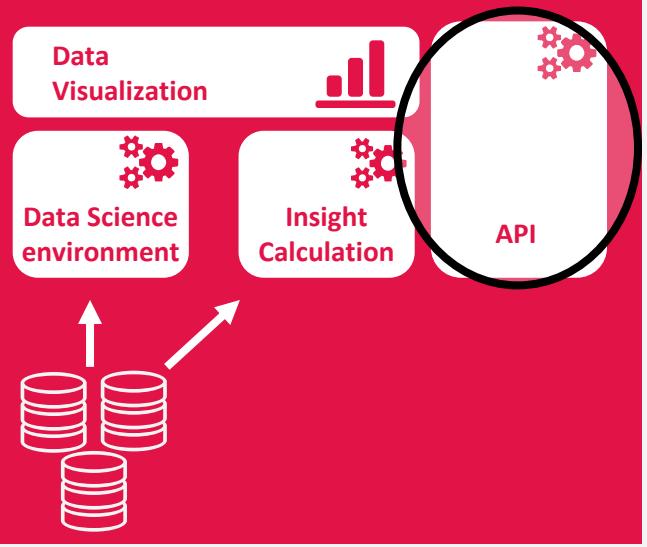
Insights are also computed in batch when new Insights are created or upgraded.

To support a large computation of different Insights on a full history, the Insight computation platform must be highly scalable. Cloud platforms are part of the solution.

- Solutions like FaaS is a good solution for real-time and scalable computation.
- Apache Spark is also a good solution for scalable computation.

Expose your data for being able to sell them

An IoT solution have different ways to distribute its Insights but the more scalable and common are API.



API

How you sell it is here – think API first

Today the market maturity for API still low but the future of IoT Market is API.

The way to distribute an Insight is an API and your customer will continue to add value on your Insight integrating them is a vertical business or by crossing them with other Insights.
This will be automatically processed in real-time thanks to APIs.

So the way you build your web & mobile integration must rely on API: you must be the first consumer of your API product.

This comes with important technical components and platforms:

- **API Management**
  - Ensure the security and control of you API
  - Allow the billing on your API
- **Developer portal & experience**
  - Make your product easy to use
  - Document your product
- **MQTT broker (or other pull solution)**
  - As there are good reasons to prefer a push integration to a pull integration

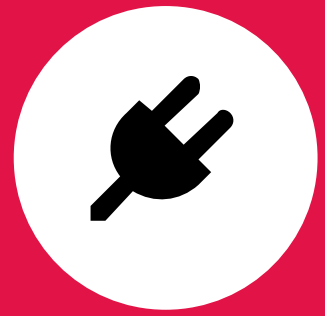
Even if API is your goal, do not forget market maturity for API is low and you may have to export CSV and other batched flat files … So you need to think about **ETL, sFTP**… technology also.

Let’s make a short break

LEARNING AT THIS STEP

Insights are the value proposition

They are created on a data science environment



Then industrialized to be computed and exposed over API

DEVICE MANAGEMENT A KEY CUSTOM COMPONENT

One in the field, each of the device will be impacted differently in the environment. This will impact its autonomy. It can make it not working or working partially. The communication conditions will also vary a lot.

The more terrible things for an IoT project is when you need to modify the hardware on field. Being able to configure or update a device remotely is important to reduce the risks. This need to be manage centrally the configuration and being able to push and follow upgrade deployments.

LOG, LOG, LOG! IDENTIFY WEAK SIGNALS

MANAGE CONFIGURATION & UPDATES

DEVICE MANAGEMENT IS CUSTOM

There is no mature software solution to manage a fleet of devices. It is a question of IoT maturity and because this is specific to each of the technology.

This is also impacting the device design.

DEVICE CONFIGURATION

Anything you can configure need to be configurable from the Device Management platform. Configuration history is an important information. Device inventory is the starting point.

SHADOW CONFIGURATION

A remote device will not immediately apply its new configuration. It can take days for devices not online. It can also be done over multiple communication requiring multiple days. During that time, the configuration need to be consistent and traced.

DEVICE LOGS & ALARMS

To understand the device condition of use and history, you need to measure extra parameters. Environmental temperature is important for many things like batteries. Specific events (like a reboot) are mandatory to trace.

DEVICE UPGRADE

Not all the network technologies allow a remote firmware upgrade. Lower the energy consumption is and lower the capabilities are. Device upgrade is not mandatory, but you need to consider it and established a plan B.

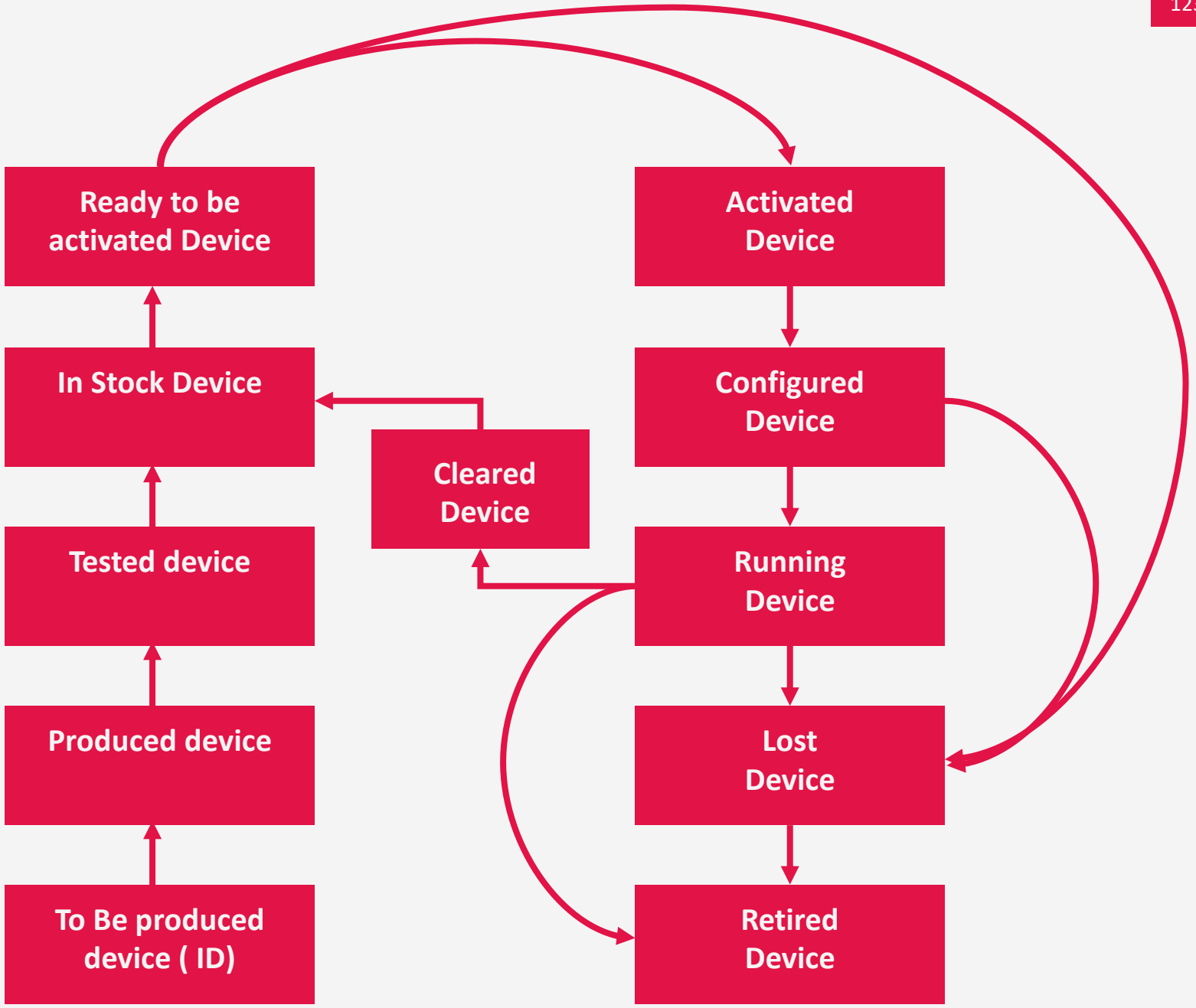
DASHBOARD YOUR DEVICE FLEET MANAGEMENT

Device fleet management is an expensive but mandatory par of your IoT solution. Without it it is impossible to scale. You need to build an efficient solution for this.

DEVICE LIFE CYCLE

The device management platform also supports the device life cycle.

This is about process: deploy a fleet of IoT devices is a supply chain & logistic question



Let’s make a short break

LEARNING AT THIS STEP

1

A fleet of IoT devices must be managed

It supports the full device cycle management. IoT device is a product you distribute, as any product company

2

This requires a dedicated tools

It’s a kind of ERP, but compared to usual product, that one is communicating, and its interest starts once you move it out of your warehouse.

3

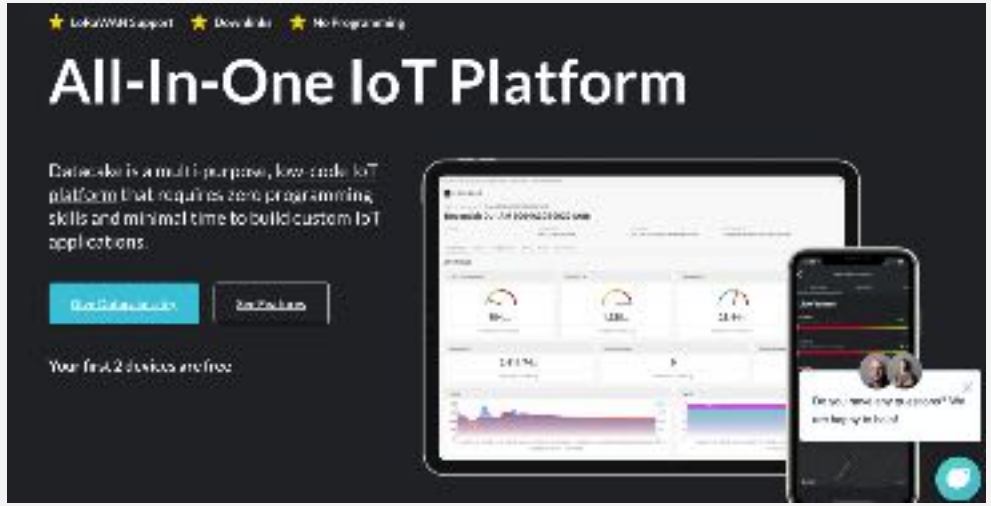
To reduce the industrial accident’s risk once in the field

Because if you need to fix anything in the field it will usually cost more than the cost of deploying a new fleet…

OUT-OF-THE-BOX IoT Platform

An IoT platform is a complex piece of software. Designing it for a project with uncertainty or a small size could be too expensive or complex.

You can find IoT platform available on the market covering partially the listed features, purchased per devices.



Why not using them ?

They are usually focusing on data visualization with limited Insight computation capability. The key features about device management are usually not implemented or insufficient. Platform is the heart of your service.

So, What are they targeting ?

They are perfect for small fleets of devices (<1000) with limited value addition, like simple tracking platforms. However, you should store your raw data outside in parallel.

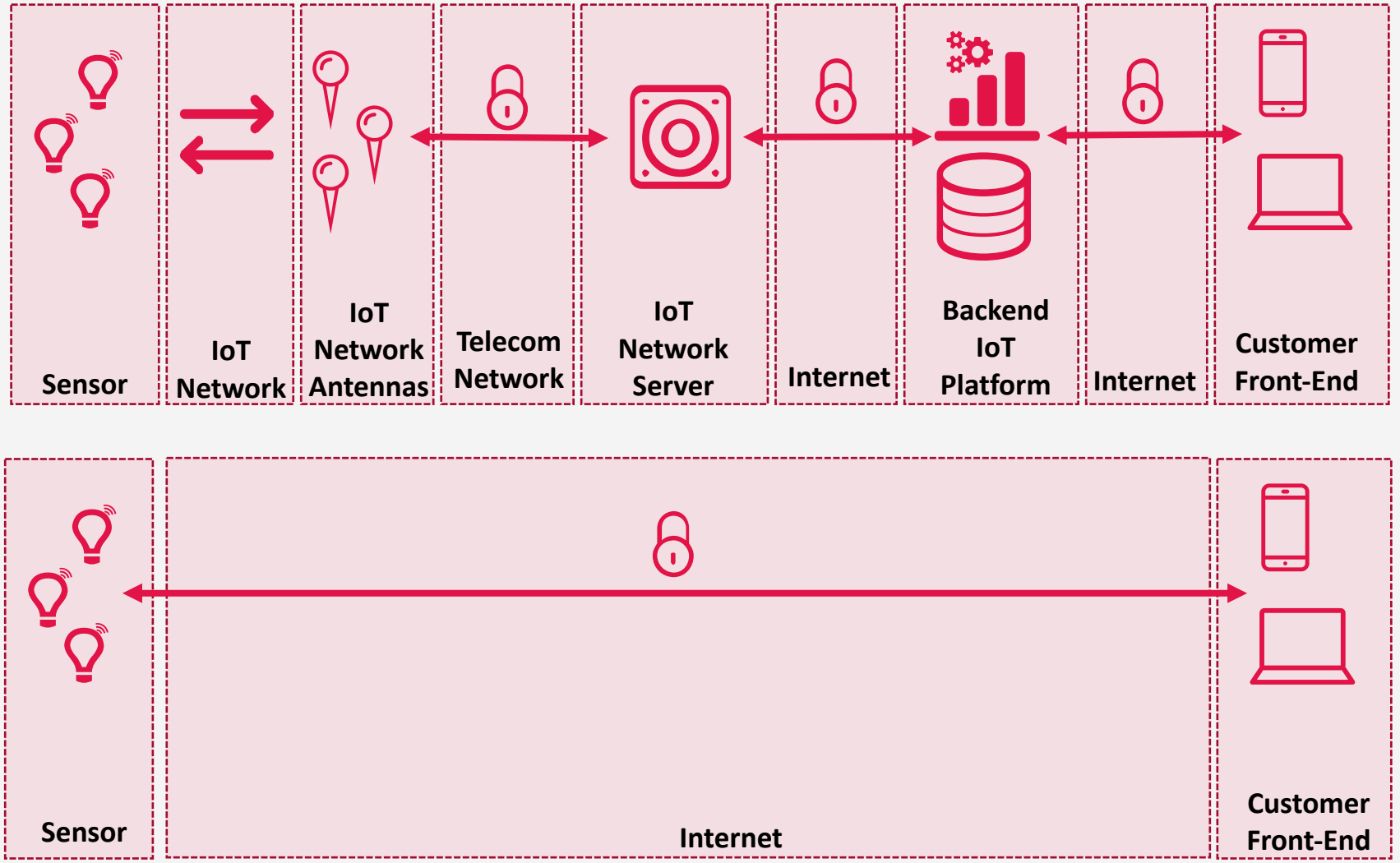
Why else, using them ?

Get online quickly for the PoC, PoT phases, make the direct value demonstration easily with limited investments.

IoT is finger pointed for lack of security, What is the truth, what to do ?

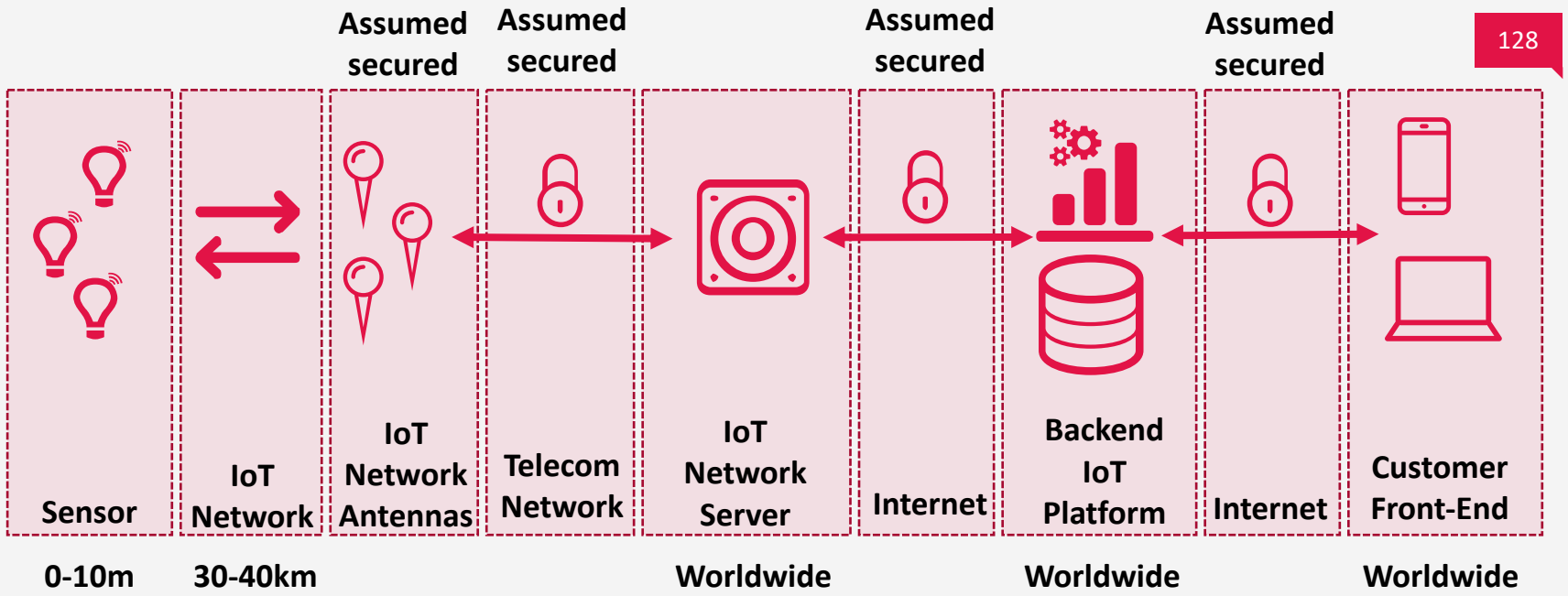
IoT Solution attack surface

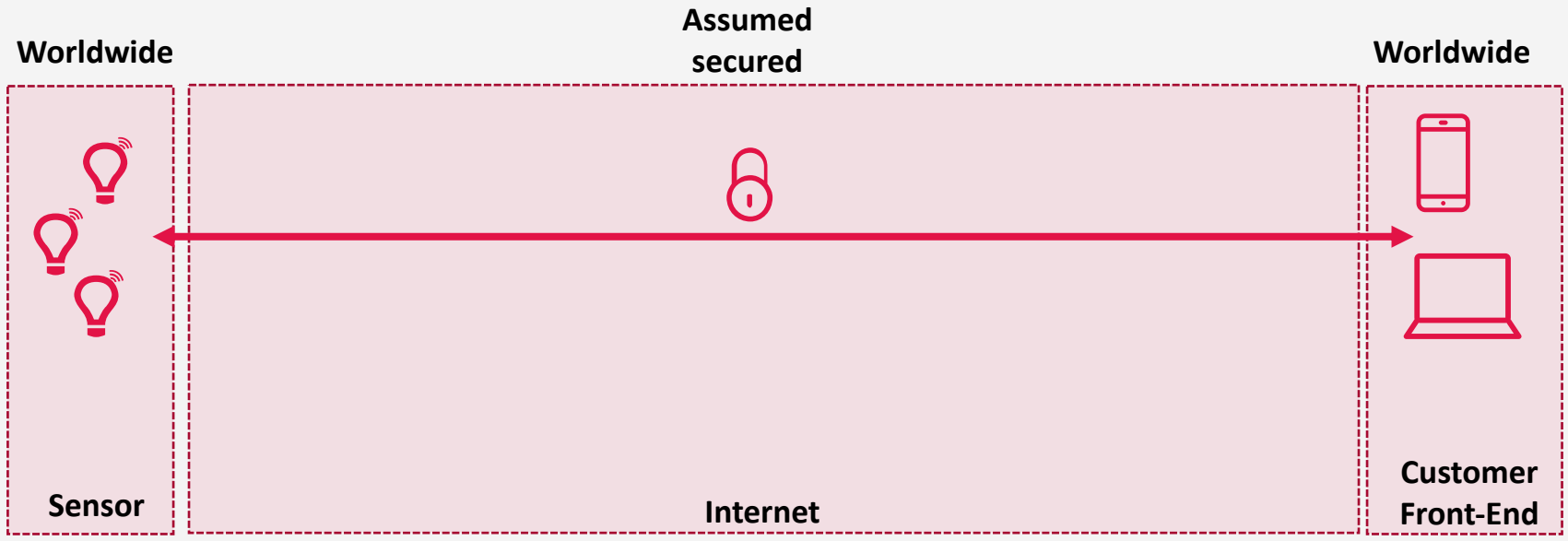
IoT security usually focus on the device security.
An IoT Solution is a wide range of components where security rules apply all along.



Attack distance weighting

Distance between the targeted element and the attacker determines the risk level and its impact. Each of the component have different level of risk that way.





This is not an IoT: this is computer with a camera. You need to secure it like a server

DIRECTLY ACCESSIBLE FROM INTERNET, WORLDWIDE

USUALLY RUNNING AN OUTDATED OPERATING SYSTEM

WITH A POOR SOFTWARE QUALITY NEVER MAINTAINED

Why ? Because it is not an IoT Solution, You've just bought hardware!

Device layer attack

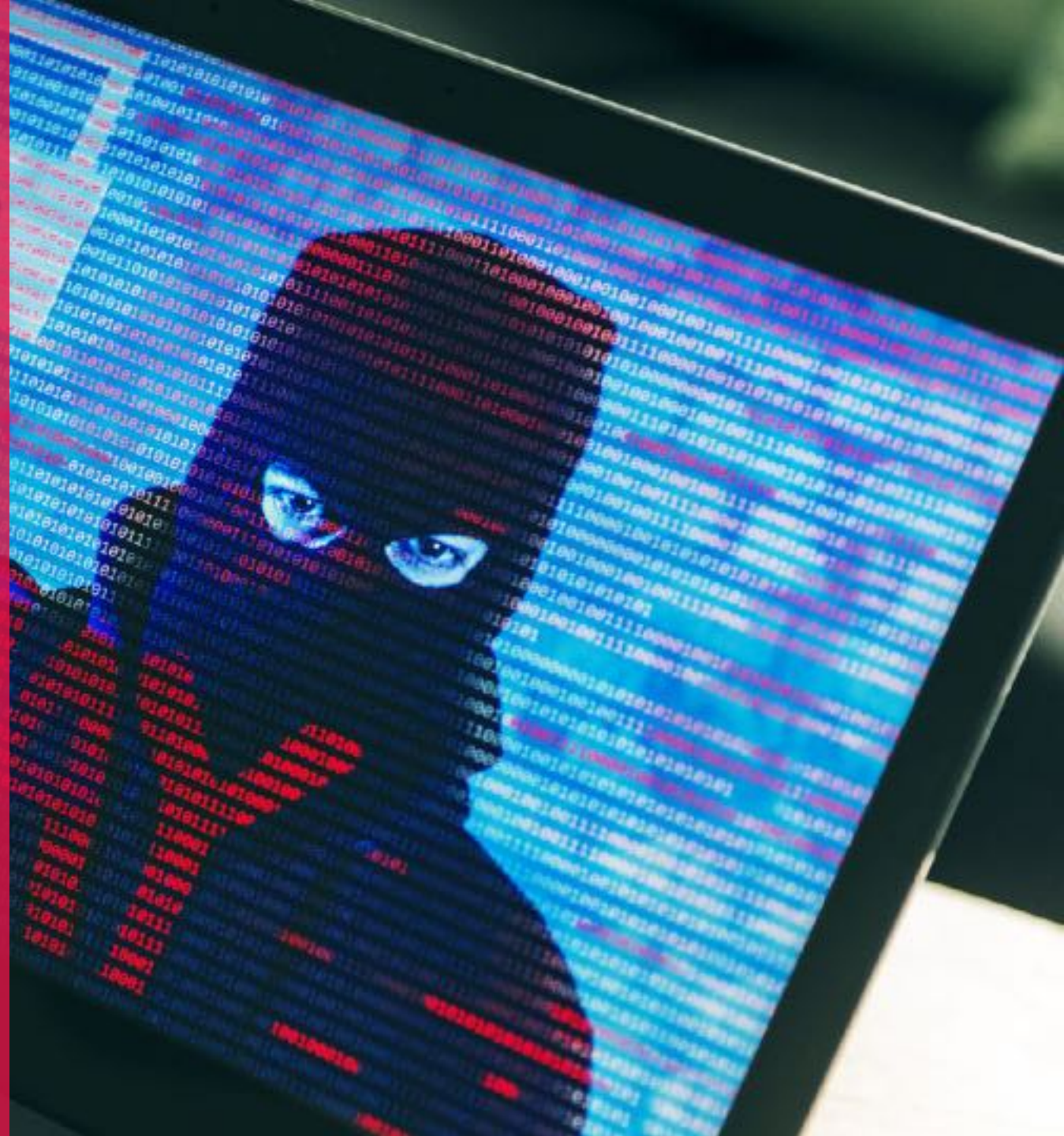
You need a physical access to the device or a near proximity. Bluetooth, Serial port … are common vectors.

HOW ?

Device Update mechanism, physical manipulation, hardware modification and addition are the classical way to attack an IoT device.

WHY ?

Ransomware, destruction, competition, data thief …
Because it’s possible or because it’s cool to talk about IoT security



A connected thermostat hacked to maintain temperature over 37°C until you pay a ramson.

Everything in the thermostat runs with **root** privileges. "**We got command injection by the SD card**, so it was a local attack," Tierney explained. "With root, you can set off alarm (and set the frequency very high) and can heat and cool at the same time."
While this was a local attack, it also isn't impossible to pull this off without gaining physical access to the device. The thermostat owner can use the SD card to load custom settings or wallpaper

A connected thermostat hacked to maintain temperature over 37°C until you pay a ramson.

DEVICE SECURITY IS PART OF DESIGN

As a device maker, you need to define the security expectations.

Security engineering cost is high and can only be handle on project start.

Define the right level, not the highest level

Practice pen-test !

1 CONTRACT FOR MAINTENANCE

Make sure your device firmware will be maintained by an internal team or an external team. Protect budget for this.

2 EXPECT ENCRYPTION FOR ALL KEYS

Any key use inside the device need to be secured. Local storage is usually sure enough, Secure elements are more for paranoid or IP protection.

3 EXPECT ENCRYPTION FOR ALL COMMUNICATIONS

Any communication shall be encrypted by default. The engineering cost at start is low. Each of the devices must use different credential. Potentially integrate different encryption solution as your device may be live for 10 years (think about WEP)

4 MANAGE YOUR IDs

Every device must have different IDs, ensure they are not sequential, not visible from outside the packaging… Make sur a successful physical attack on one device will not allow remote access on all other devices.

5 PROTECT FIRMWARE AND REMOVE DEBUG BACK DOOR

It is common to have an unprotected device with firmware possible download or developer backdoor for debugging phase. Ensure you close them all.

IoT Network Attack

This kind of attack is possible short range and allow a certain level of security for the attacker. Depending o, device feature you can steal data or gain control of the devices.

HOW ?

By listening the device communication as radio wave are accessible for all.
By faking the device or network to communicate with device or IoT platform

WHY ?

Get access to industrial secrets, track people or assets. Destroy industrial machine, rob a house…
Also to attack you brand is a competitive market

Only trust your code !

Listening radio wave is nothing you can prevent.

LoRaWan is easy to listen but the traffic is encrypted… until it's broken

Sigfox is complex to listen (existing solution only work around 2 meters)… until it is becoming easy.

1

APPLY THE NETWORK ENCRYPTION CAPABILITIES

All the modern radio solution have an encryption layer. You need to enable it or request developers to consider it.

2

NEVER CONSIDER NETWORK ENCRYPTION SECURED

Even if these solutions are secured today, nothing make you sure it won't change in the device lifetime duration (10 years). Just think about WEP …

3

IMPLEMENT YOU OWN END-TO-END ENCRYPTION

Add an applicative END-TO-END encryption. This will add a protection if the network standard is broken. This will also protect your data against a Network Server data leak. (more probable than a device being listen, with larger impact)

4

MANAGE ERRORS AND WEAK SIGNALS

There are multiple ways to attack a system from the network. You should track weak signals like communication loss, reboot, sequence rupture, frame with invalid key received…

Let’s make a short break

LEARNING AT THIS STEP

1

SECURITY IS PART OF THE DESIGN & COSTS

Ensure you manage the security at the beginning of the project

2

SELECT THE RIGHT LEVEL OF SECURITY

Identify the risk exposure, find a good compromize and trace your decisions

3

ENCRYPT EVERYTHING SENSITIVE

There is no reason to not encrypt local keys, communications… so just do it

LPWAN Sigfox & LoRaWan Technologies in detail.

2 French technologies

3

sigfox

- Created in TOULOUSE (FRANCE) in 2009
- FRANCE fully covered since 2013
- Found rising
  - 15M€ in 2014
  - 100M€ in 2015
  - 150M€ in 2016
- Hardware device solution from most of the silicon vendors
- 72 countries deployed and seen as a single global network (as of Nov. 2020)

LoRaWAN™

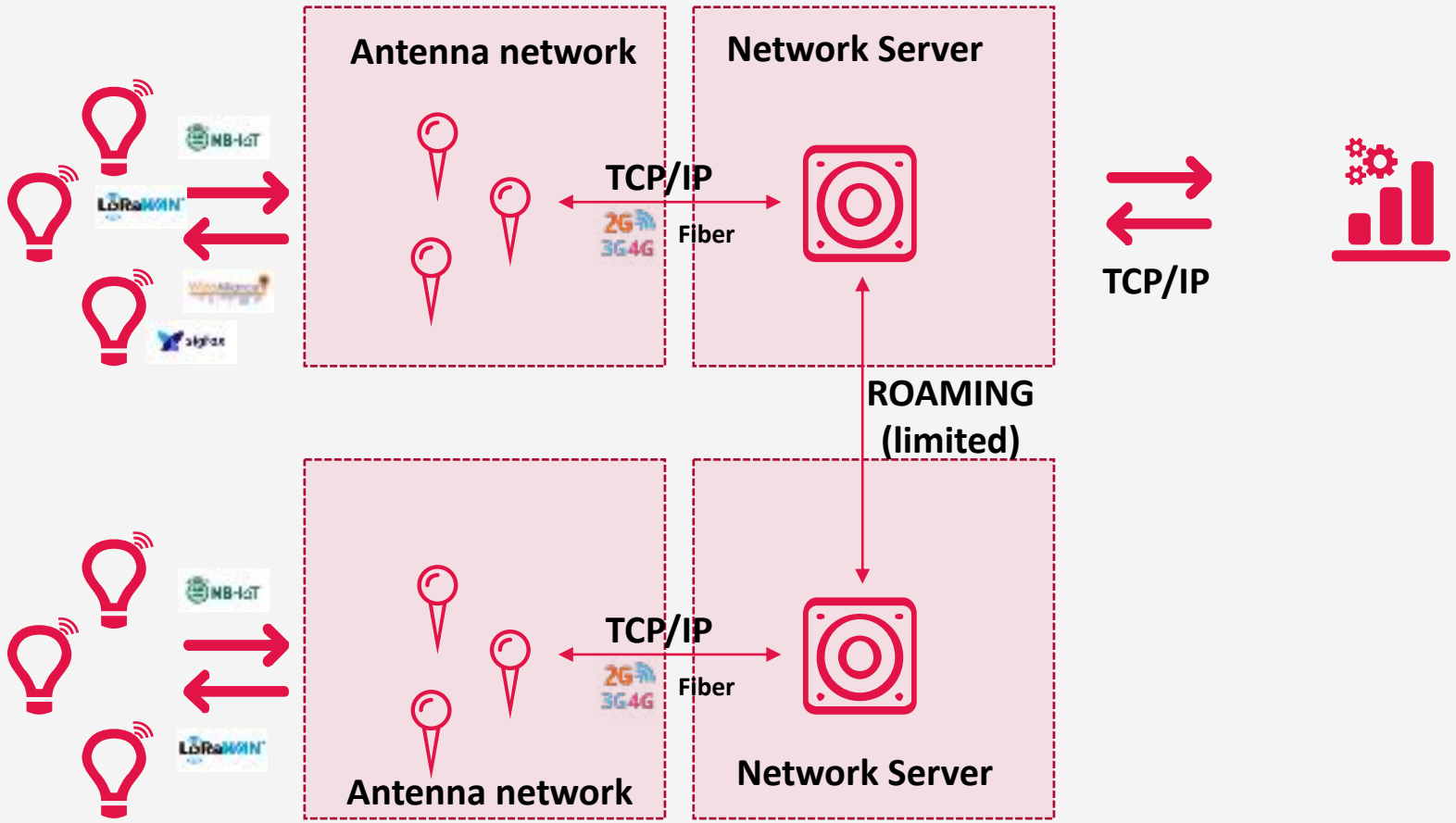
- Created in GENOBLE (FRANCE) in 2009
- Acquired by SEMTECH in 2012 for a price range between 5M$ and 25M$
- SEMTECH is a Silicon vendor with an exclusivity. 1 licence acquired by St Microelectronics.
- LoRaWan 1.0 released in 2015
- Deployed by about only 5 telecom company nation wide.
- Thousands of private networks
  - TTN – crowdsourced global network
  - HELIUM – crowdsourced global network as a blockchain

LPWAN have a common architecture

The devices messages are captured by multiple antennas around.

The antennas forward the messages to a network server owned by the network operator (private or public)

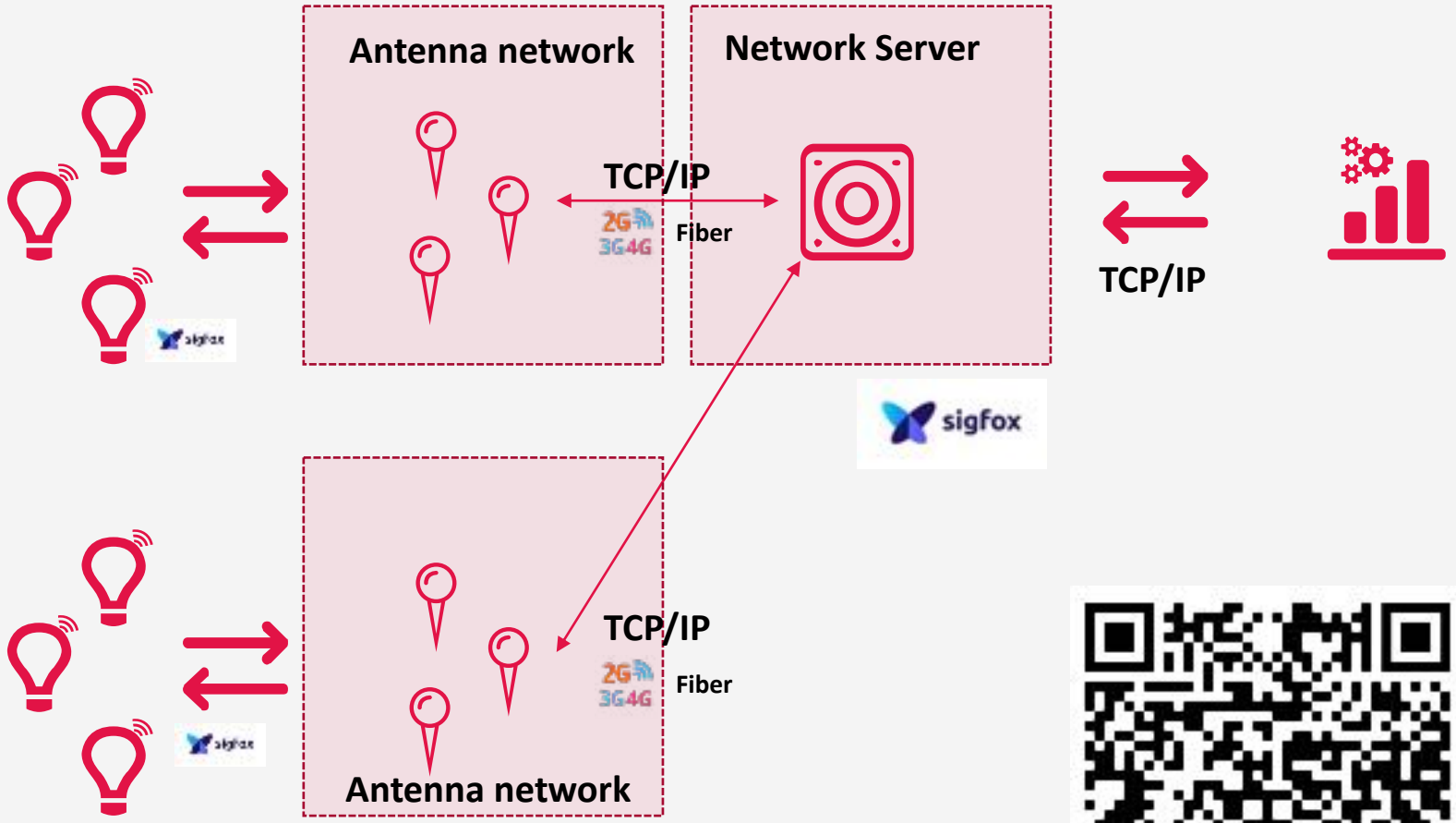
Then the network server transfers the payload to the custom backend, eventually, roam it to another network server.



LPWAN have a common architecture

Sigfox is a particular case with a World-Wide network and a single Network Server

70 countries
1.1B people



4

Save power: don’t be connected

Compared to classical communication network, LPWAN are using non connecter mode. It means a device can deep sleep for month, wake up, fire a message and back to sleep.

This means a lot of power saving and a strong resilience against jamming.

Network do not have edge access control, but centralized control managed by network server.

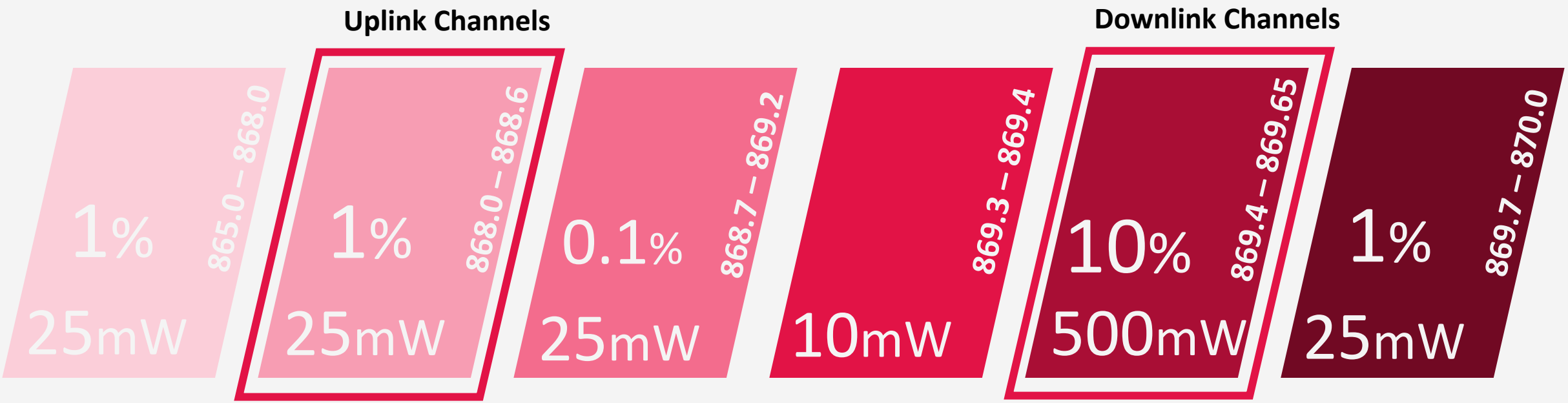
Shared radio band

SIGFOX & LoRaWan are using ISM bands, they are free for use in condition you respect rules defined by the regulation. This regulation differ in the different zones. The purpose is the same, share the radio band in a balanced way between the user.
In Europe, the rule is to limit communication to 1% of the time per device. In North America it's to not transmit on the same channel for more than a given time.

9

European regulation on 868MHZ ISM band

865Mhz-870 Hz



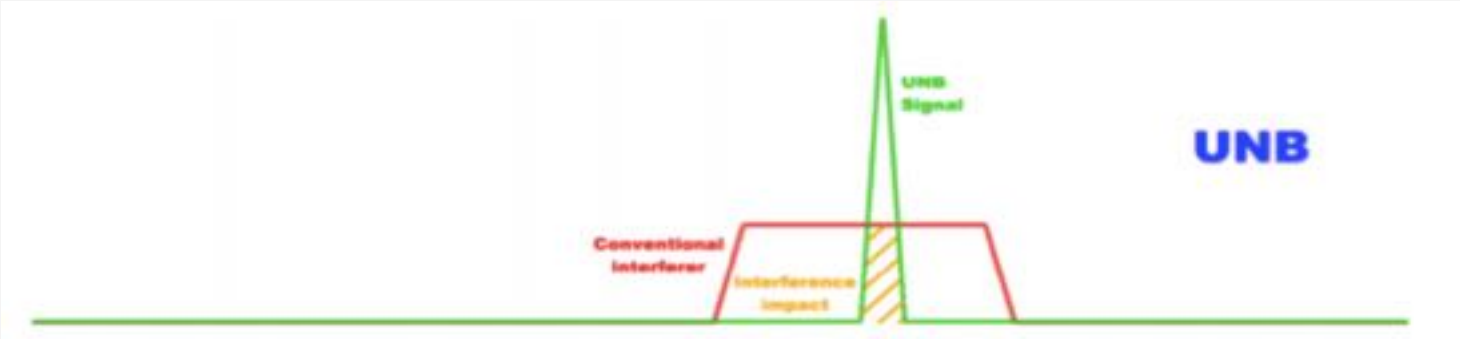
European regulation is defined by different laws like ERC-REC-70-03E for EUROPE and the application in FRANCE is based on ARCEP 2012-0612 and 2014-1263 published on JORF 30/01/2015.

It limits the transmission time for any equipment to a certain percentage of the time during a sliding hour. This proportion of time depends on the frequency band. This is what we named DUTY-CYCLE. This is the percentage value in the above description. It also limit the transmission power.

https://www.disk91.com/2017/technology/internet-of-things-technology/all-what-you-need-to-know-about-regulation-on-rf-868mhz-for-lpwan/

Etre entendu sur de très longues distances malgré le bruit ambiant

2 approches différentes pour 1 même objectif



SigFox – Ultra Narow Band

Emettre un signal sur une bande de fréquence la plus fine possible pour ainsi maximiser la puissance en un point et passer au dessus du bruit.

LoRa – Etalement de spectre

Emettre un même signal sur plusieurs fréquences pour « contourner » les bruits

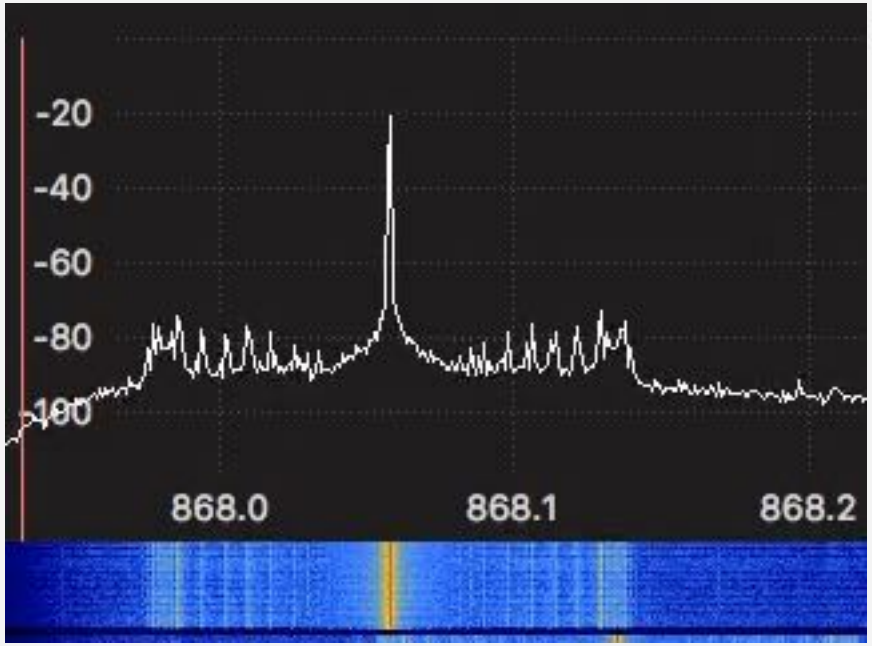
sigfox

Is an asymmetric technology

The technology use for transmitting data is simple when the technology required to receives Sigfox messages is highly complex and based on Software Defined Radio.

Is a symmetric technology

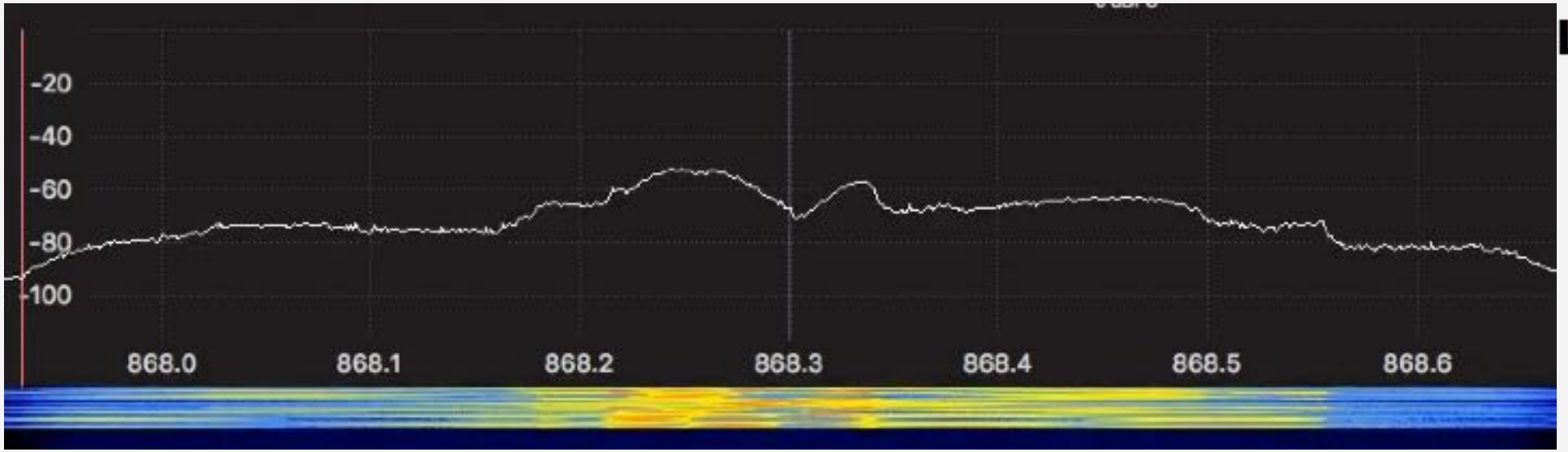
Transmission and reception are based on the same technology and complexity level.



sigfox

The radio technology is totally different for reaching the same goal

7



LoRa

https://www.disk91.com/2017/technology/internet-of-things-technology/learn-about-sigfox-and-lora-radio-technologies/

Let’s make a short break

LEARNING AT THIS STEP

1

LPWAN SIGFOX & LoRa ARE 11 YEARS OLD NOW

Both has been created in FRANCE and now deployed all over the World

2

THEY RELY ON ISM BAND TO BE DEPLOYED AT LOW COST

This means respecting regulation rules in place to share the ISM band between all the different technologies using it.

3

THE TECHNOLOGIES BEHIND ARE DIFFERENT

But they are reaching the same goal: allowing to communicate over long distance with a minimum of energy

Sigfox, one IoT network to cover the entire World

sigfox

6

An asymmetric network

The technology use for transmitting data is simple when the technology required to receives Sigfox messages is highly complex.

A Software Defined Radio Network

Simplicity and efficiency

ISM BAND (free of access)

Use of 868MHz band in Europe, Africa. 902MHz -920 MHz in North, South America and Asia. In each of them the exact frequencies differ.

LOW POWER / WIDE AREA

With only 14dBm in Europe, the coverage is 60km. Distance record was 1023km from Spain to Eire in 2016. Only 1000 antennas allows to cover most of a country like FRANCE. Compared to 4000 for LoRaWan and 50.000 for 4G

LOW THROUGHPUT

Transmission is limited to 100 **bits** / seconds in Europe and up to 600 **bits** / seconds in North America. This is related to the different regulations.

FIXED PACKET LENGTH

User payload limited to 12 byte per frame. Only available options are 0, 4, 8, 12 bytes.

BI-DIRECTIONAL

Devices can receive message from the network (DOWNLINK) up to 4 times a day, right after an uplink communication. A device can request more than 4 downlink per day. Other are best-effort only.

REGULATION APPLICATION

The application of the regulation is under the device maker responsibility. You can transfer up to 6 consecutive frames in Europe if you want.

Sigfox over the technology

Sigfox is at first a global, world-wide telecom operator. Here is a big part of the innovation.

A single device can communicate all over the world without roaming consideration.

Sigfox is deployed in many countries and growing fast

- 72 countries in November 2020
- 5,7M KM2 covered
- 1.3B people covered
- 16M devices connected in 2019

X2 on every 18 Months since 7 years

Reduced “Time to get the first fired frame”

As everything is already defined in the protocol, in a developer perspective, the time to getting started with the Sigfox technology is short. Device design is also simplified and regulation difference have a limited impact in most of the use-cases.

Security and reliability

MESSAGE SIGNATURE

All the messages are signed with an EAS processed and indexed. It proves the emitter identity and allow to reject usurped or replayed messages in a 4096 messages cycle.

ENCRYTION

Clear payload is the default setting. AES-CTR can be activated when the devices has been designed for. It is part of the standard Sigfox lib. Sigfox is complex to receive for real: open-source receivers are only working under 2 meters.

JAMMING PROTECTION

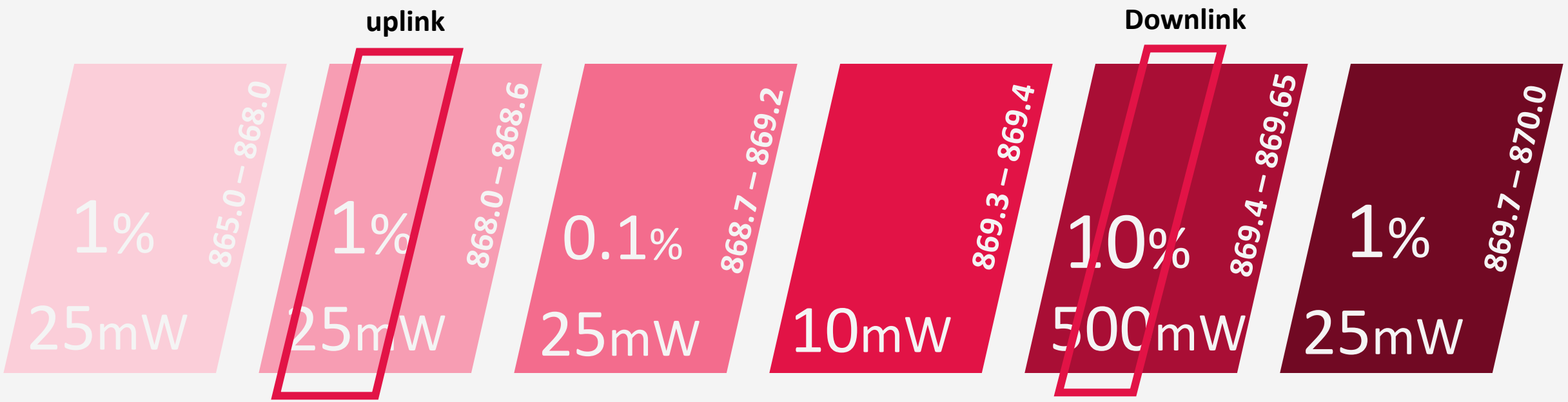
As Sigfox doesn’t require any reception for firing a message it’s really complicated to JAM it. This is one of the reason it has been chosen in Securitas solutions. To jam Sigfox you basically need to jam the different base-station around… forget it.

COMMUNICATION RELIABILITY

Every frame is replicated to get 3 transmissions of the same message on different frequencies. It allows a 99.99xx deliverabilty is the covered zones.

European regulation on 868MHZ ISM band

USE OF 865Mhz-870 Hz

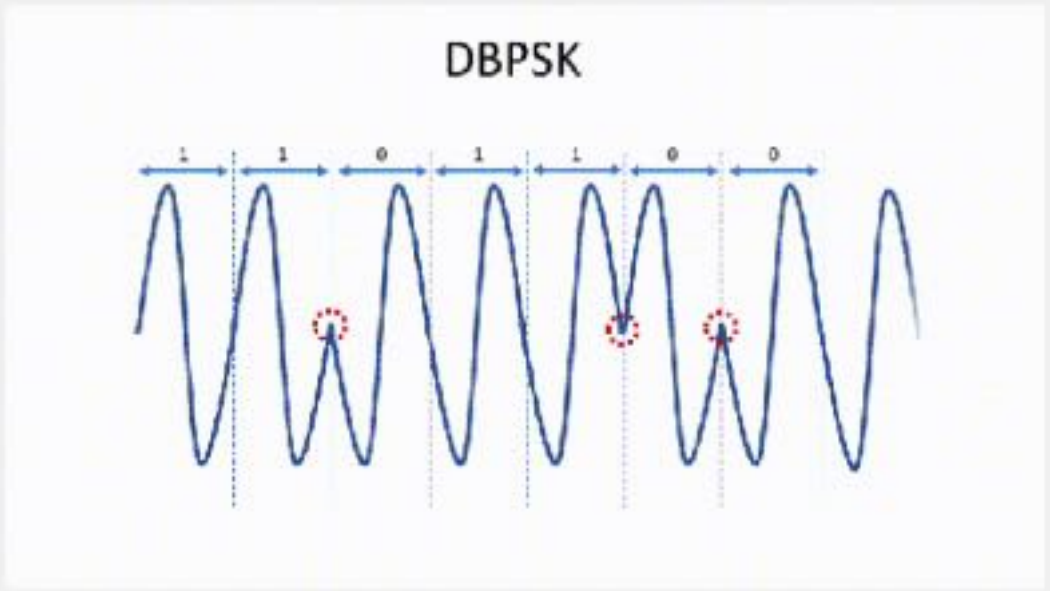


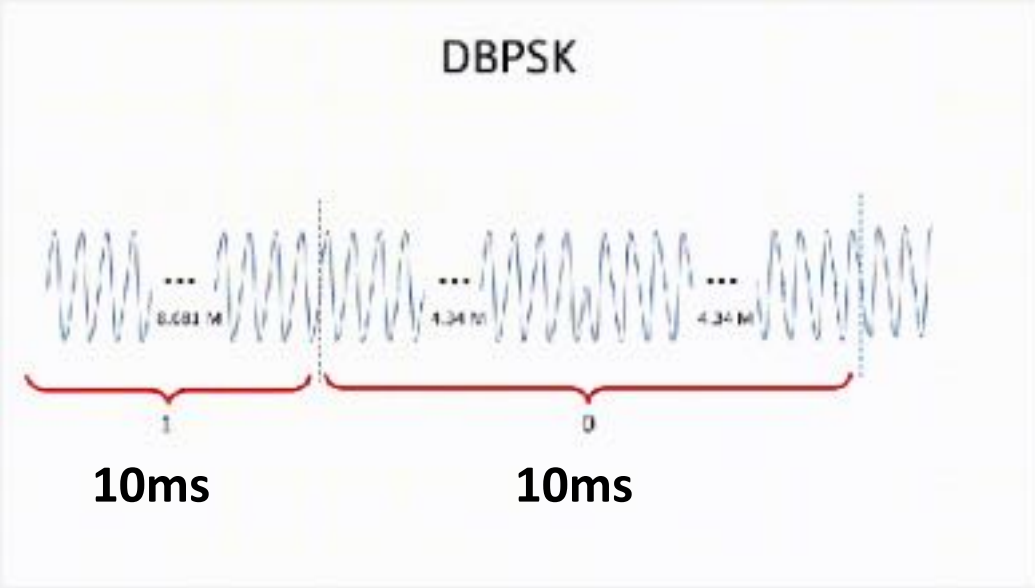
Sigfox only 200KHZ. In Europe it is centered on 868.130MHz. In these 200KHz there are 2000 channel, each of them have a size on only 100Hz

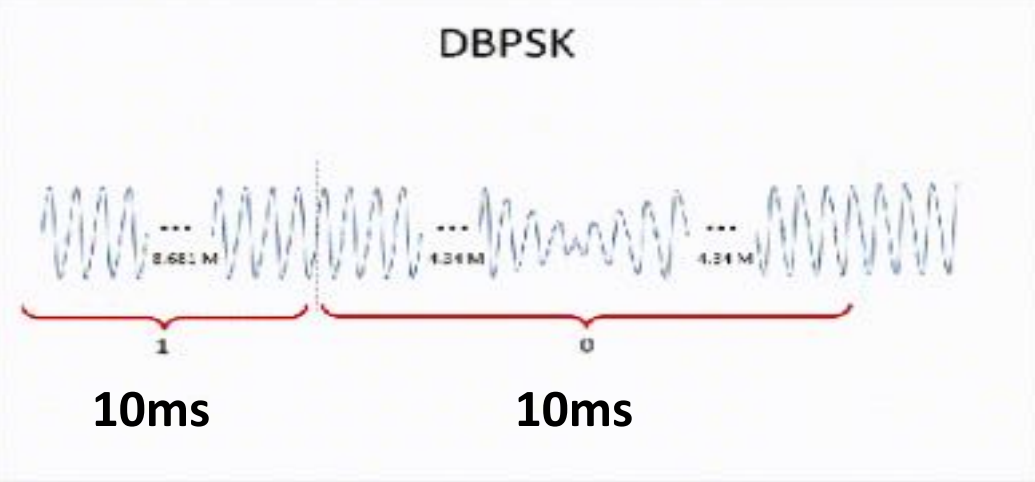
DOWLINK are using a 10% duty cycle band for two reasons:
- A base-station responds to many different devices
- The radio situation for a base-station is better than for a device. You need more power to be received by a device.

SigFox – Transmission radio sur DBPSK

Differential Binary Phase Shift Keying







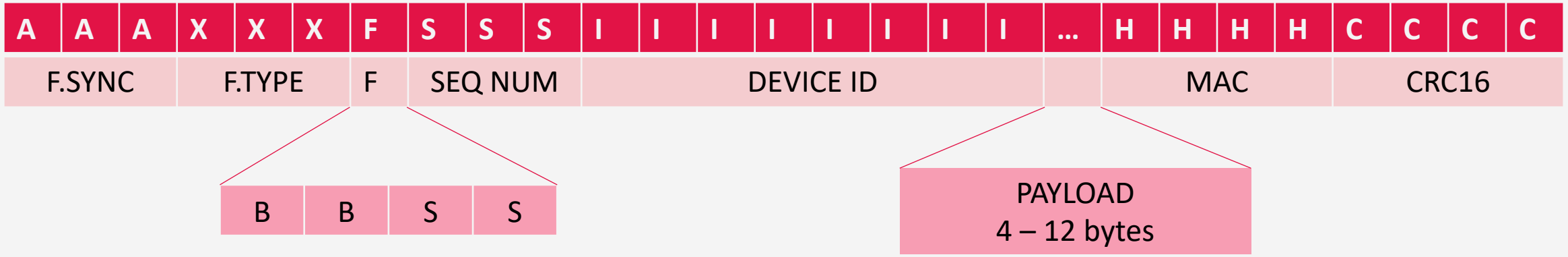
Temps d'une trame:

- 12B : 2,08s
- 8B : 1,76s
- 4B : 1,44s
- 1B : 1,2s

8

Sigfox – Uplink data frame format

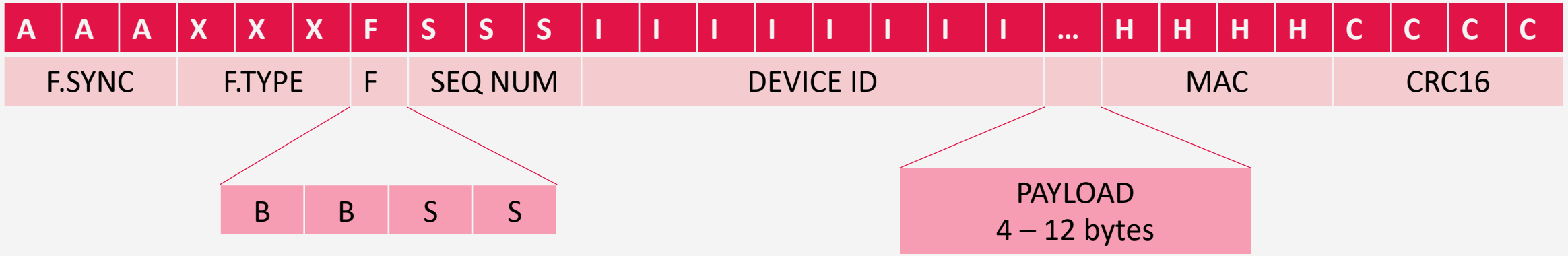
1 single type of frame skeleton for all the communications



F.SYNC : Preamble – 20 bits 01010101010101010101 – clock sync and Sigfox message identification
F.TYPE : Frame type (related to payload size and repeat)
F : Flags : Flags (bit value, downlink, byte added in payload)
Seq NUM : Sequence number, incremented on every communications
Device ID : device address, uniq
Payload : User data
MAC : CBC-MAC Signature based on NAK (Network Authentication Key)
CRC16 : Frame bit validation

Sigfox – Uplink data frame format

1 single type of frame skeleton for all the communications

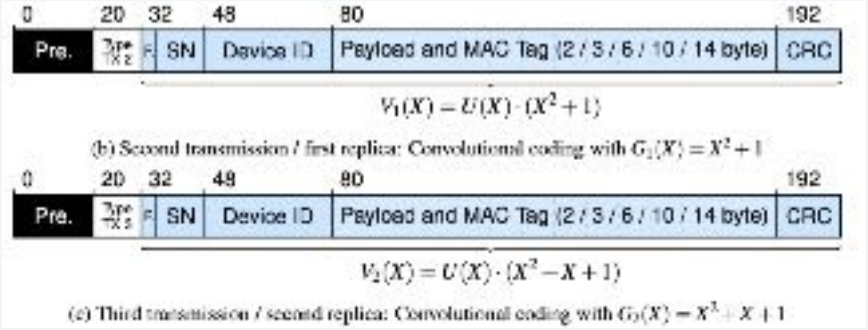


The medium PAYLOAD is identified by the F.TYPE Field / each of the repeat have a different encoding

- **0 bit/byte - 06B 6E0 034**
- **1 bit - 06B 6E0 034**
- **1 byte - 08D 0D2 302**
- **4 bytes - 35F 598 5A3**
- **8 bytes - 611 6BF 72C**
- **12 bytes - 94C 971 997**

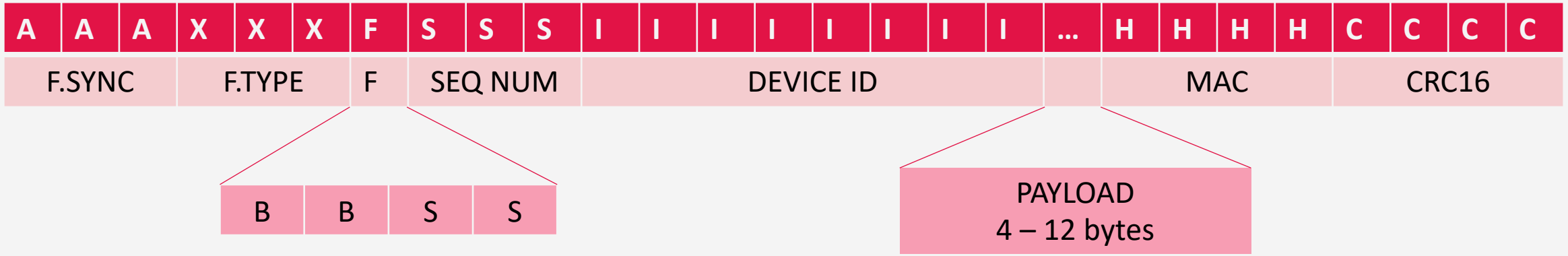
1st frame is sent with no specific encoding

2nd and 3rd frames use Convolutional Codes



Sigfox – Uplink data frame format

1 single type of frame skeleton for all the communications

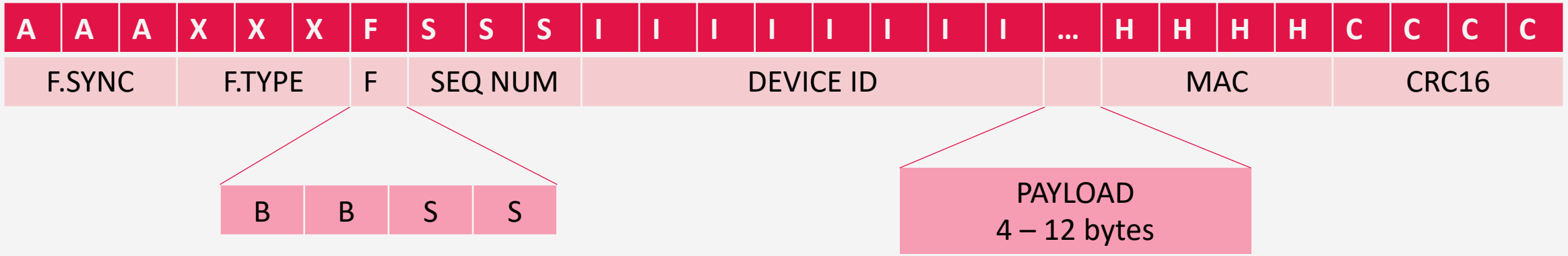


Flags have the following content

- **BB**
  - **0 bit / byte frame** **00**
  - **Single bit frame** **10 (value 0)** **11 (value 1)**
  - **Others (00 to 11) can be read different ways:**
    - **Number of MAC byte added in payload field**
    - **Real size of the payload = payload size – BB**
- **SS**
  - **00 – uplink frame w/o downlink**
  - **10 – uplink frame w downlink expected**

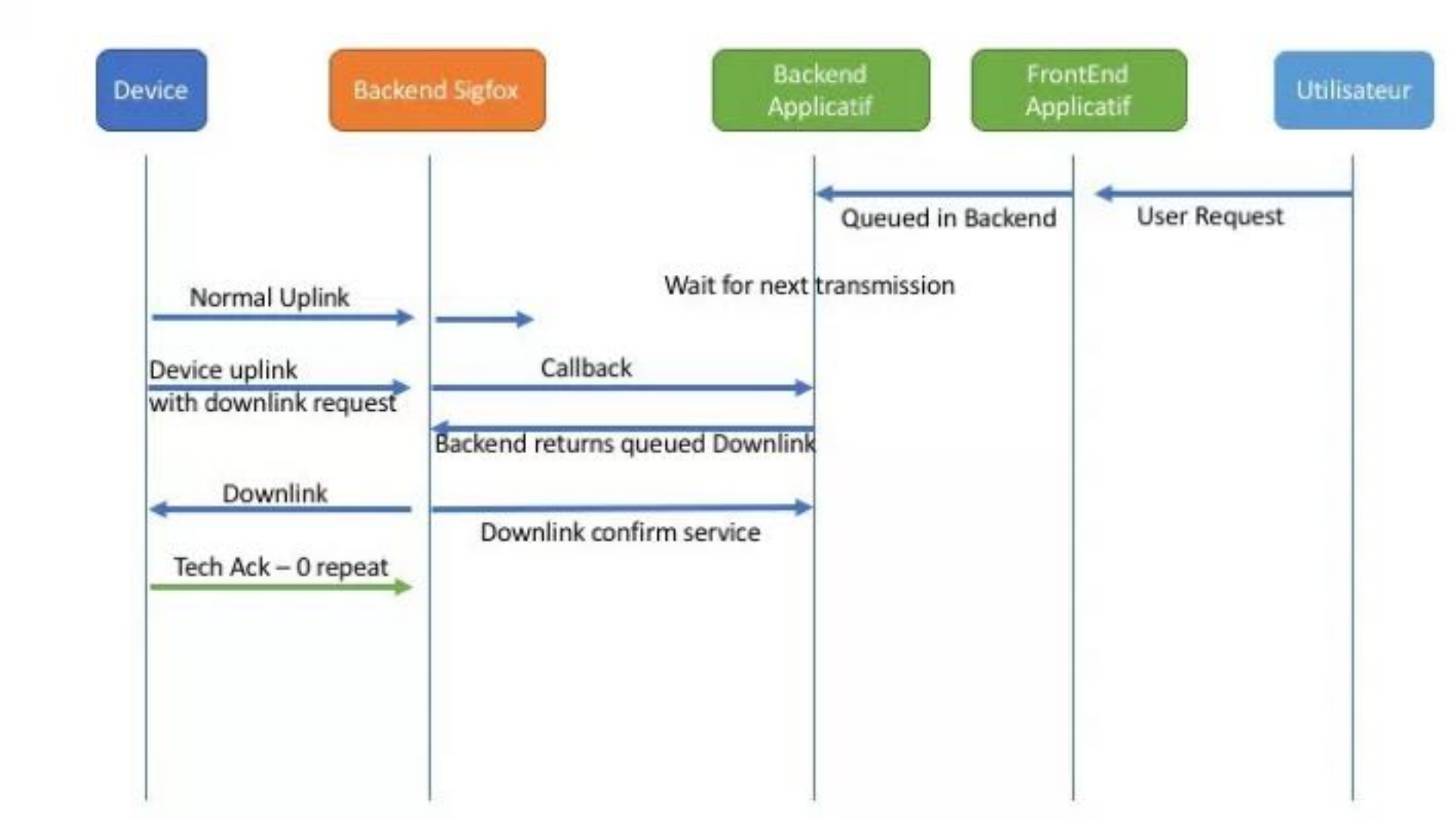
Sigfox – Uplink data frame format

1 single type of frame skeleton for all the communications



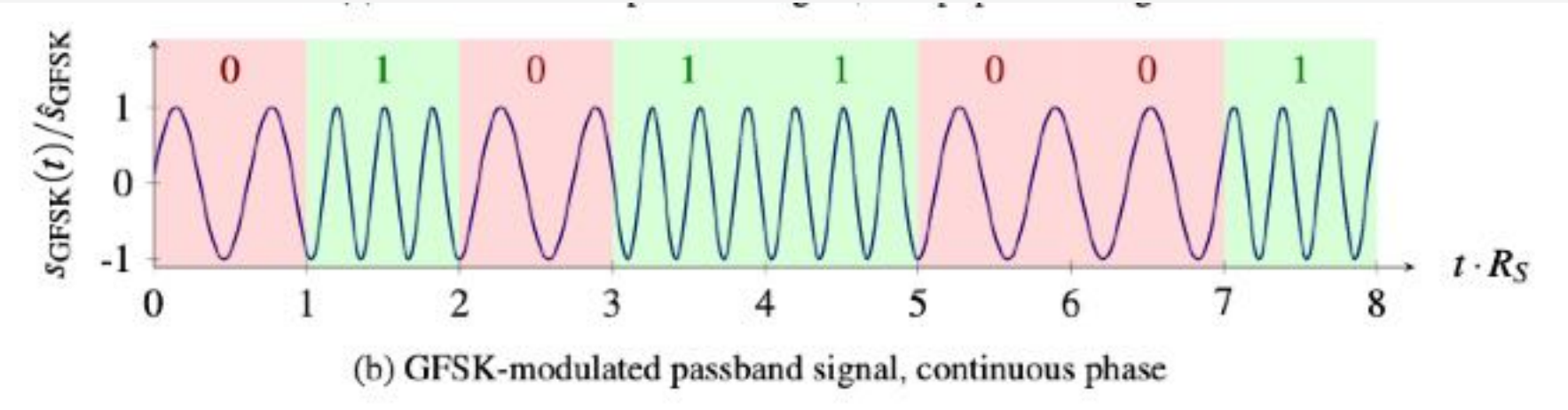
- **MAC computation use a secret KEY (NAK) shared between device and Sigfox backend.**
- **MAC includes F, SEQNUM, DEVICE ID, USED PAYLOAD**
- **MAC computed with EAS-128-CBC, only a part of the result is kept to create the MAC (from 2 to 5 bytes)**

Sigfox – Downlink communications



SigFox – Downlink transmission is GFSK

Gaussian Frequency-Shift keying (because a device can't receive DBPSK)



(b) GFSK-modulated passband signal, continuous phase

Symbol rate

- 600 Bit/s

Frequency

- Determined from the uplink message frequency

It works long-range because

- Frequency is 869.4MHz to 869.65MHz
- So the transmission power is 500mW

Sigfox – Downlink Frame

Sent by the network on downlink request

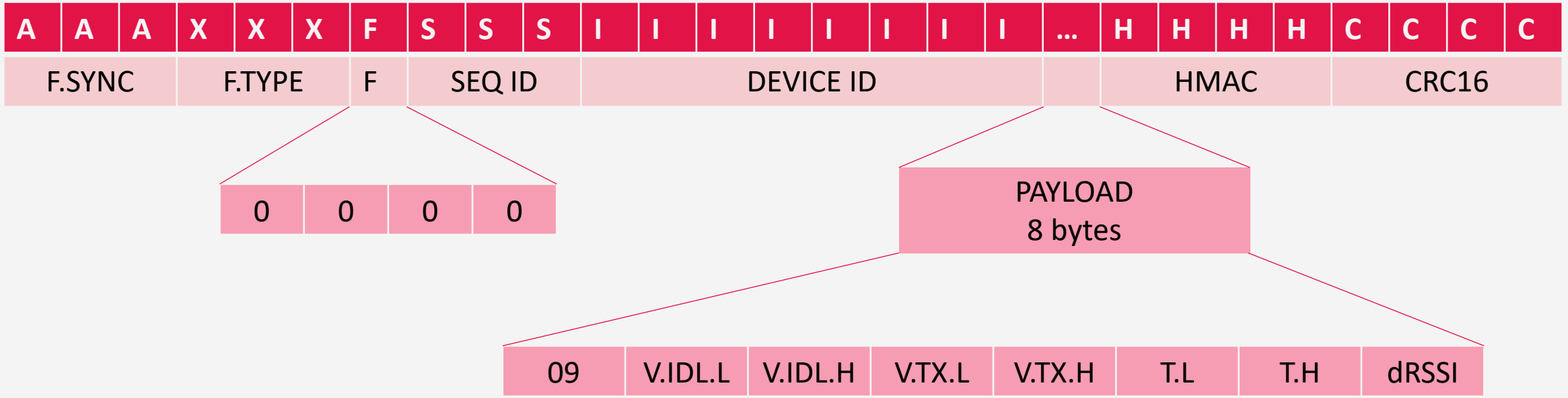
PREAMBULE – 0x2AAAAAAAAAAAAAAAAAAAB227
EEC – Error correction, redundancy information
Payload – Downlink Data
MAC – Authentication for the destination, EEC + PAYLOAD
C – CRC-8

Destination is not identified in the DOWNLINK frame:
Any device can read the downlink frame, only the one knowing the NAK used to compute MAC will resolve the MAC challenge correctly. That way, only one device will consider the frame as valid.

That way, 4bytes of transmission are saved, collision risk is reduced.

Sigfox – Frame RX OOB (downlink confirmation)

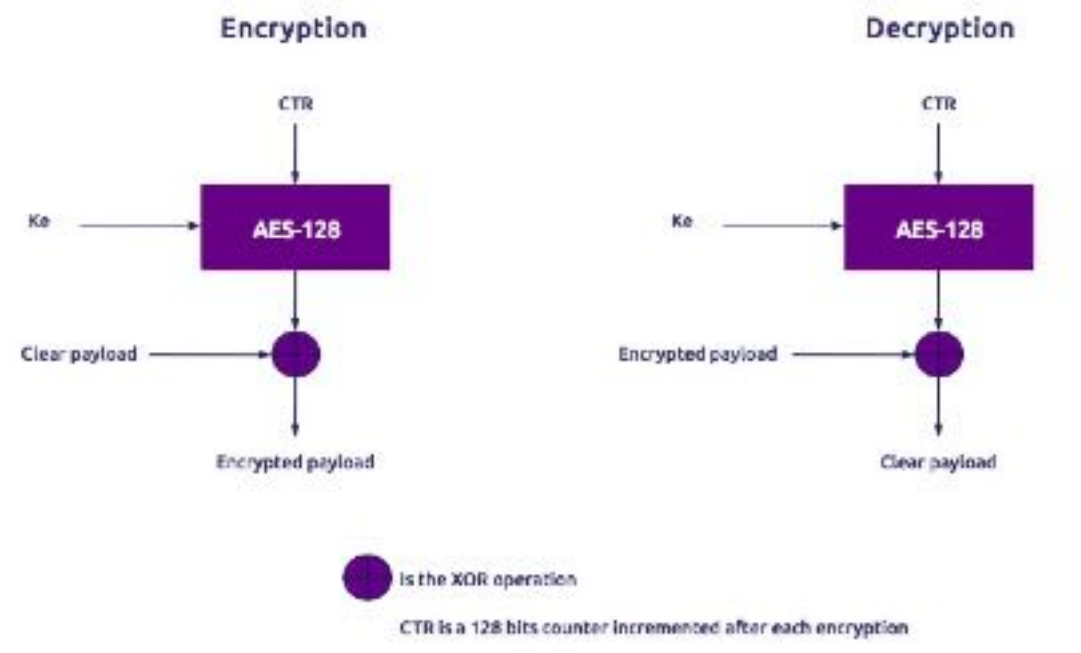
Sent by the device on downlink reception as a confirmation (no repeat)



V.IDL : Idle voltage
V.TX : Voltage during the last Sigfox transmission
T : Temperature
dRSSI : Downlink reception signal level

Sigfox – Frame encryption (uplink & downlink)

Activable per device, request to be made at Sigfox



The solution is equivalent to LoRaWAN encryption.
- The Ke is not negotiated but derivates from the Device ID and NAK.
- CTR is composed by a derivate vector from DeviceID and NAK + the addition of a 16bits Sequence ID

- The AES(KE,CTR) gives a different key for each communication (modulo 65536). This key is a source for an XOR operation with the frame bits.

Encryption protects against data listening over-the-air. It also protect against replay attack.

10

11

Sigfox get benefit of a large ecosystem with hundreds of available devices and tons of device-kit.

Standard radio chip + MCU price starts about $1.5 / Ultra low-cost solution starts at 0,20€ for radio + MCU solution.

https:// partners.sigfox.com

https:// makers.sigfox.com

Devkit includes 1 year of communication

Sigfox has been used to closely work with the startup eco-system even if in the last year they are most focusing on big company & at scale projects

SIGFOX NETWORK SERVER

13

Also call Sigfox backend. It receives messages and help IoT solution administrator to manage the subscription and device fleet.

Network server is where you link your device with your final application.

TRACKING USE-CASES

The main Sigfox use-cases in volume are in two domains:

- Security
- Assets tracking

In the domain, Sigfox propose a solution to get a device localization from a single frame based on received radio signal or WiFi signals around. This avoid using a GNSS chip for getting a location.

Precision and compliance vary:

- 1km to 20km for received radio signal
- 30m for WiFi signals when exists

This option is ATLAS.

THE THINGS NETWORK

LoRaWan, many IoT networks deployed on your own

LoRaWAN™

A POINT-TO-POINT RADIO COMUNICATION TECHNOLOGY

A NETWORK RUNNING OVER LoRa.

LoRa Numbers (as of Nov 2020)

180.000.000

LoRa compatible transceivers already distributed by Semtech

1.000.000

LoRa based gateway chips sold

This could cover 1,5x the total earth surface and 5x the surface where human live. But the real coverage is … 1-2% ?

POINT-TO-POINT RADIO TECHNOLOGY

ISM BAND (free of access)

Use of 868MHz band in Europe, Africa. 902MHz -920 MHz in North, South America and Asia. In each of them the exact frequencies differ. Each channel is 125KHz large.

LOW POWER / WIDE AREA

With only 14dBm in Europe, the coverage is 15km. Distance record was 832km from a balloon (cheating). Only 4000 antennas allows to cover most of a country like FRANCE.

LOW THROUGHPUT

Transmission is limited to 250 **bits** to 5400 **bits** / s depending on Spread Factor choice, for 125kHz bandwidth. Can be 11kbps for 250KHz.

VARIABLE PAYLOAD LENGTH

User payload can be 59 to 250 bytes depending on Spread Factor and regulation. FCC have a maximum authorized time in the air.

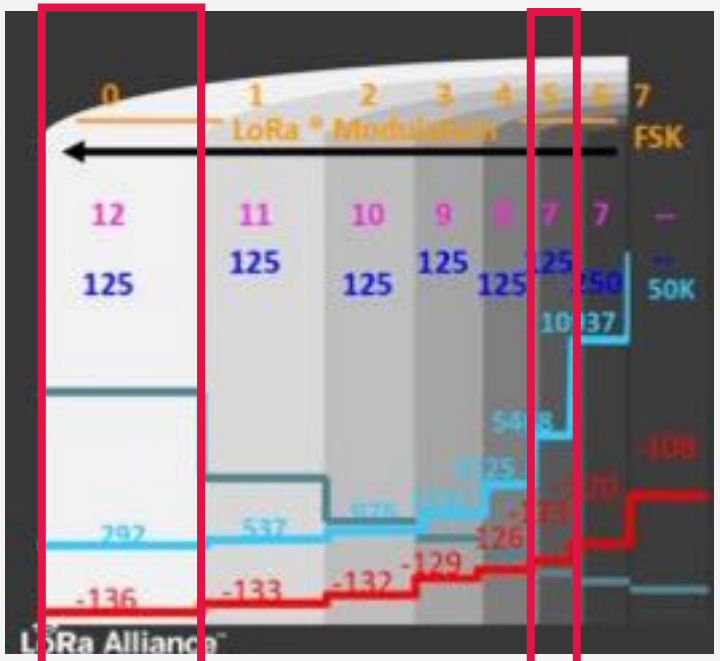
BI-DIRECTIONAL

Devices can receive message from the network (DOWNLINK) right after an uplink communication. Downlink messages are used to ack transmission and to transfer data to the device. Firmware update capability, in certain conditions, has been proven.

REGULATION APPLICATION

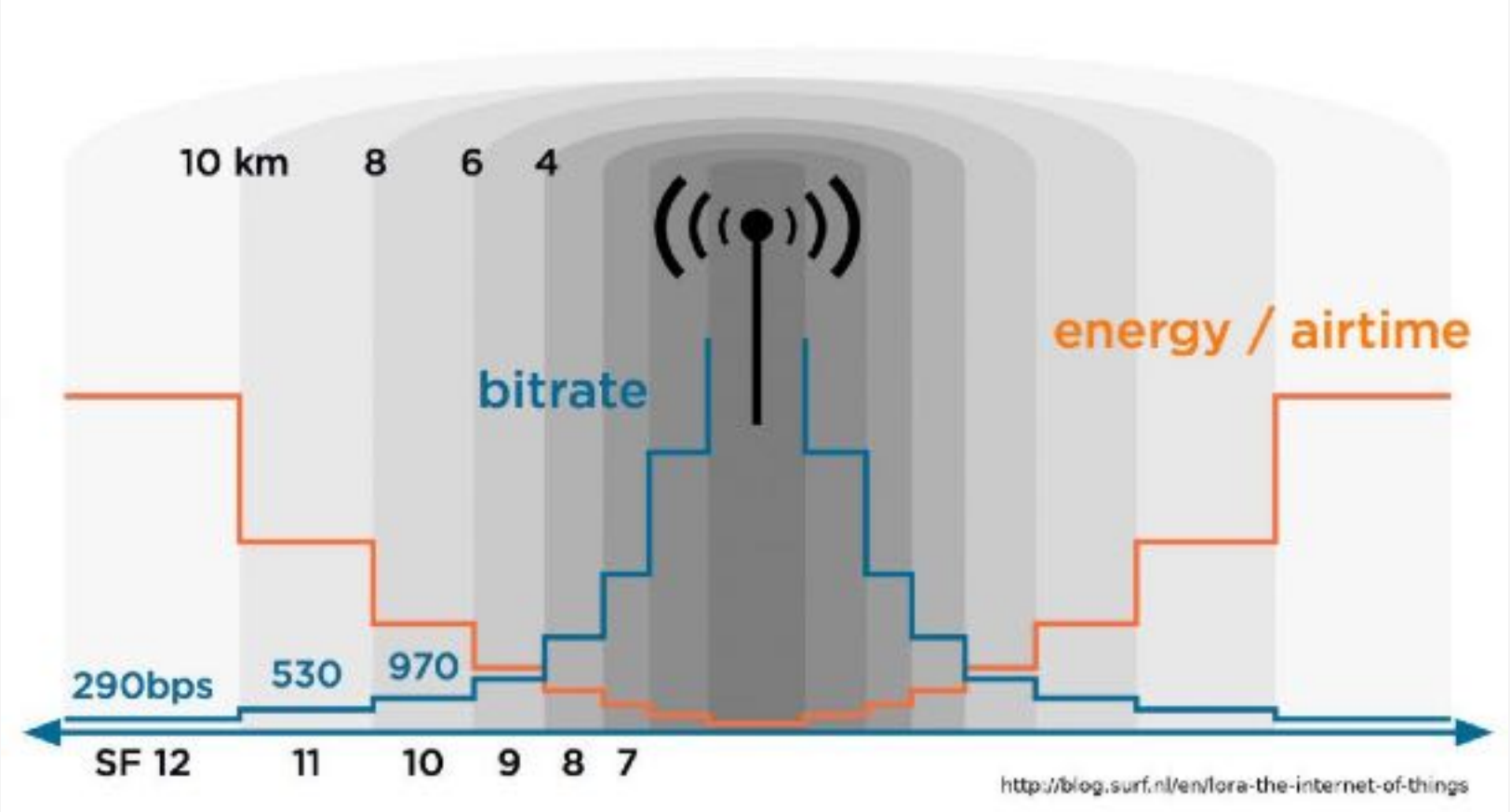
Usually, the regulation rules are managed in the LoRa and LoRaWan stacks. Therefore, what you can do depends on the implementation and the zone you are.

SPREAD FACTOR – SPEED AND COVERAGE



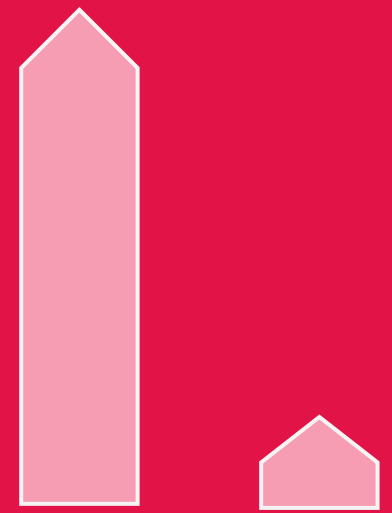
SF12
250bps
-136dBm
sensitivity

SF7
5400bps
-133dBm
sensitivity



HIGHER SPEED – HIGHER DATA FREQUENCY

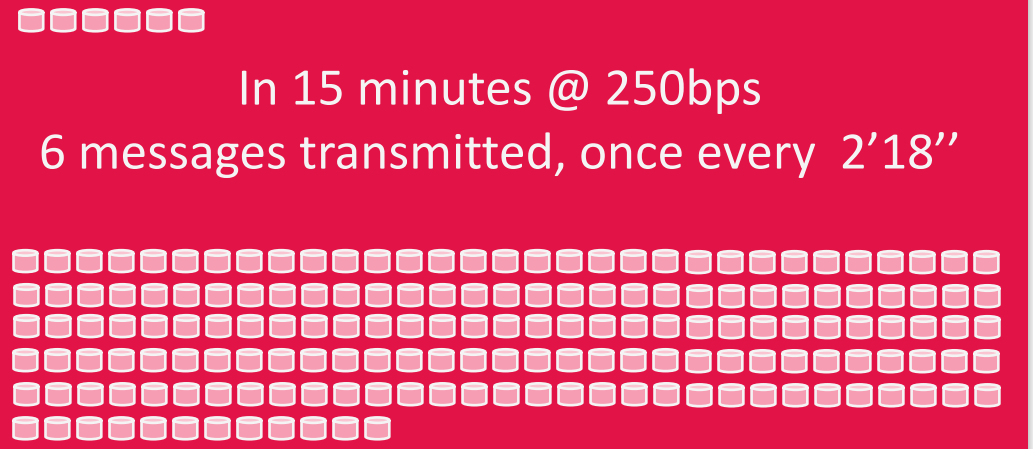
Time to transmit 10-bytes of data



250bps
1,4s

5,4Kbps
56ms

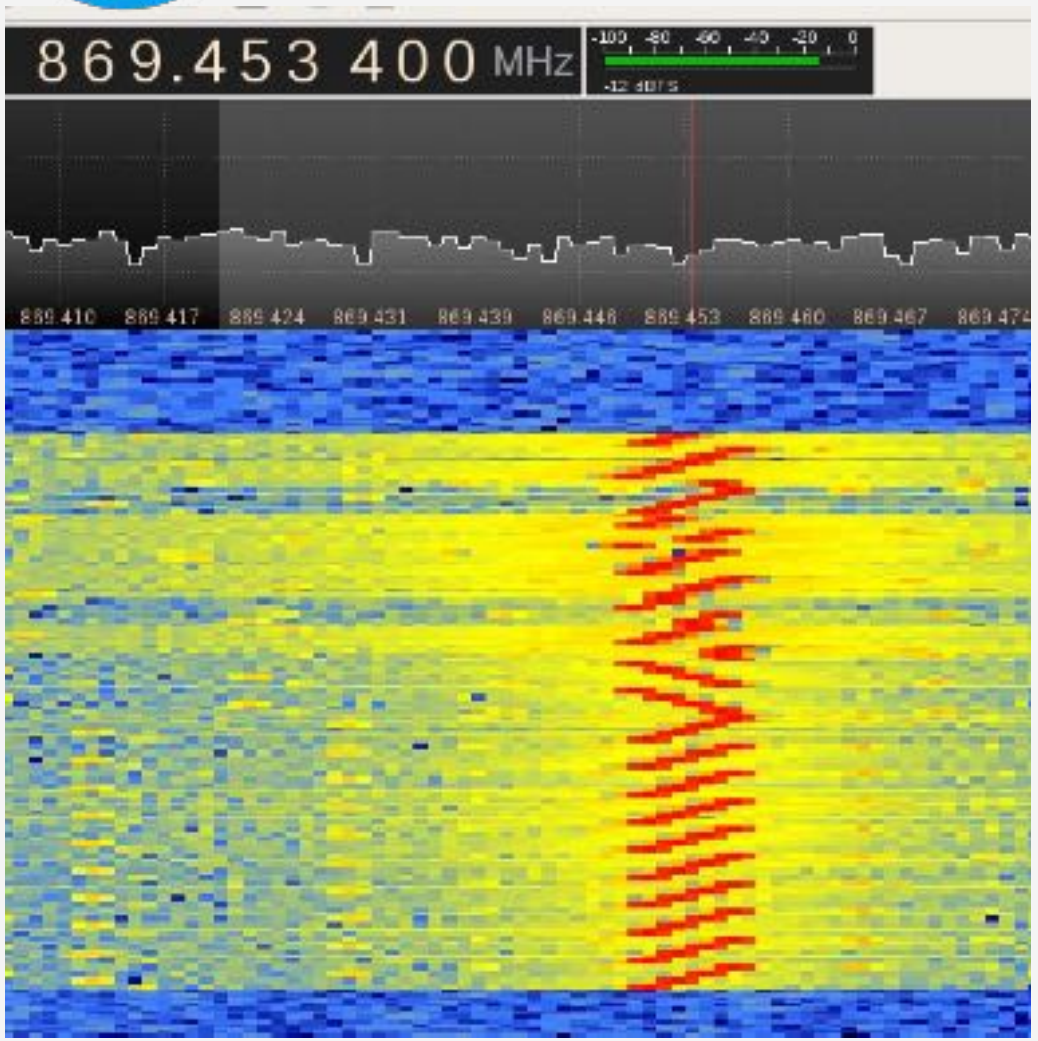
Transmission period for a 10-bytes message (in EU)



In 15 minutes @ 250bps
6 messages transmitted, once every 2’18’’

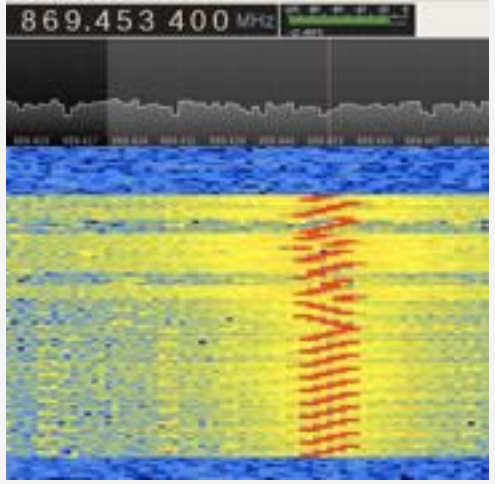
In 15 minutes @ 5400bps
162 messages transmitted, once every 0’5’’54

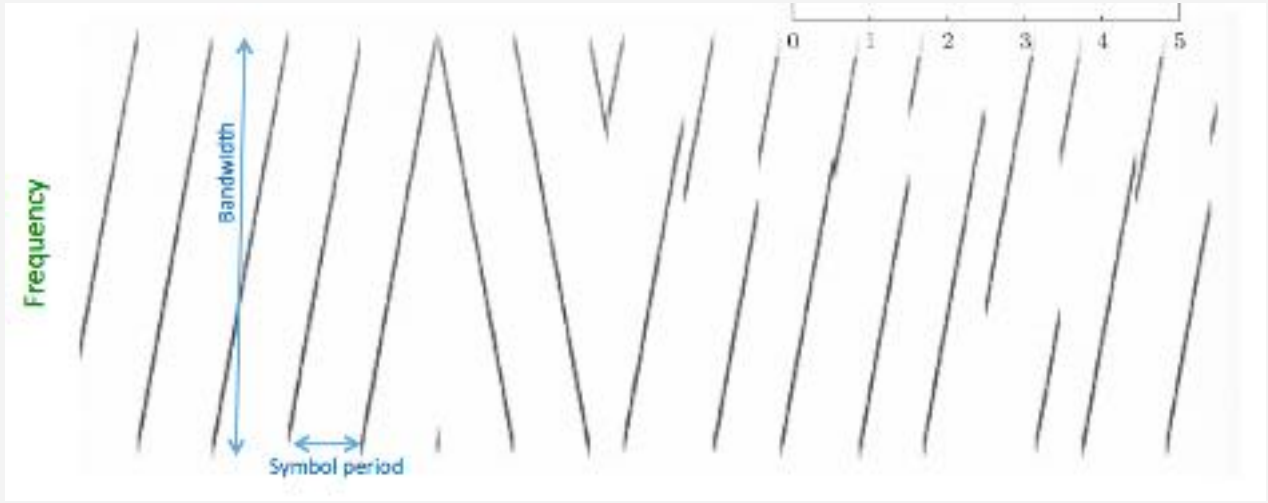
RADIO MODULATION PRINCIPLES



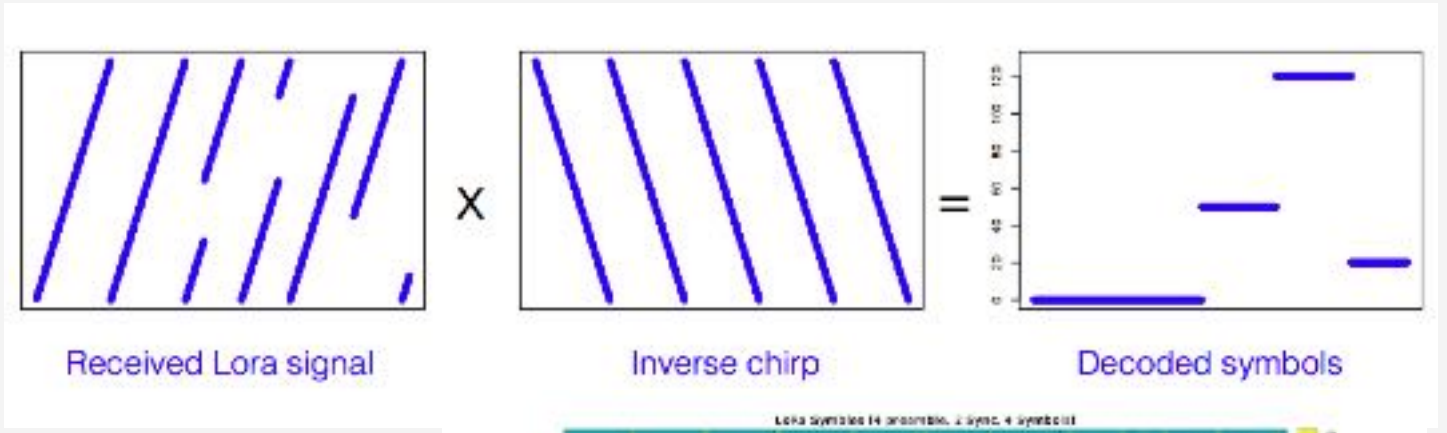
Data are transmitted by shifting the radio signal frequency. This movement creates a pattern encoding the data.

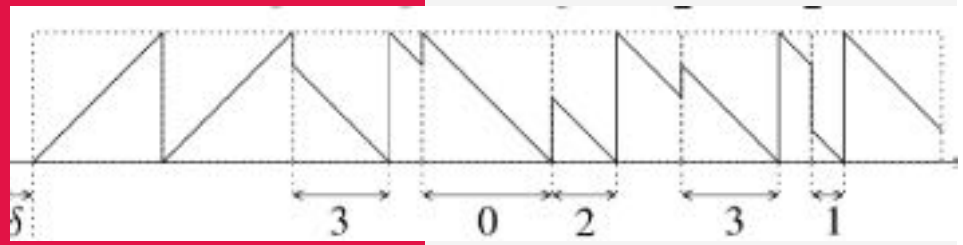
Any other noisy signal in the middle of this movement will be ignored.

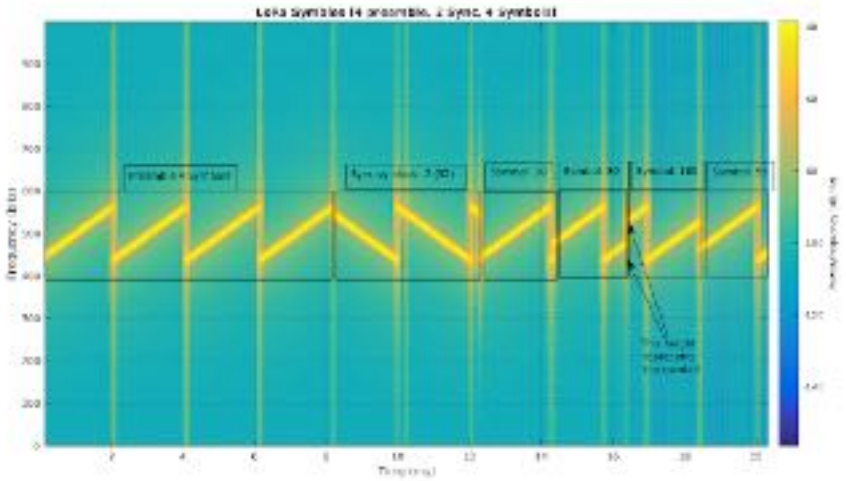


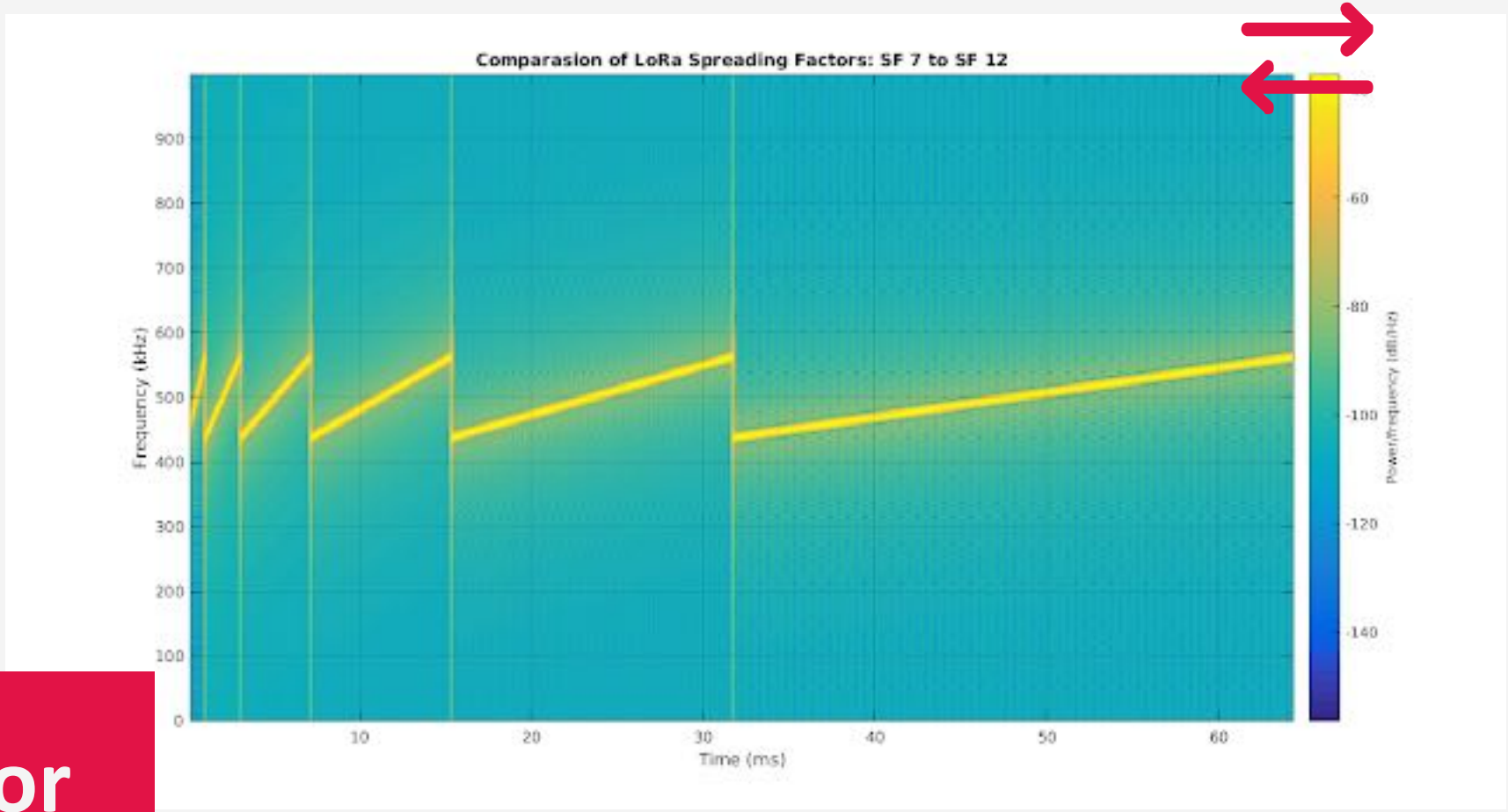


LoRa Symbol decoding principle









LoRa Spread Factor principle

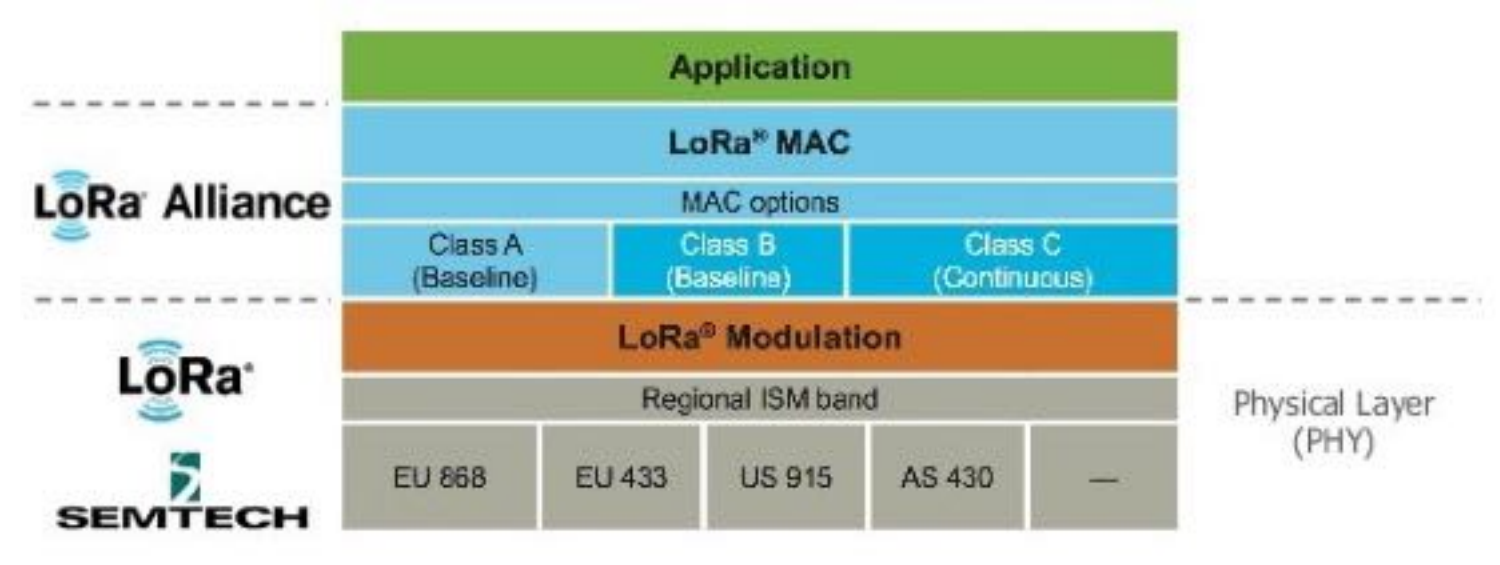
Getting more time to execute the frequency movement pattern allows a better decoding over noise. Better distance achieve, less loss, but lower throughput

LoRaWan is one of the existing network implementation for LoRa.

Amazon SideWalk is another implementation of LoRa to build a network.

LoRa is also widely used in point-to-point application.

LoRaWAN



LoRa Wan

Use LoRa layer 2 communication and add a protocol on it to support a network integration with different devices and gateways. This can be compared with a TCP/IP layer with many differences.

LoRa

Point to point communication, we can compare LoRa with WiFi in terms of network layer.

Network layer

LoRaWAN is a specification defined by LoRa-Alliance (telecom operators and industrial companies, 500+ actors) since 2015.

It defines one of the way to create a network over LoRa with the ability to support multiple public operator in each area

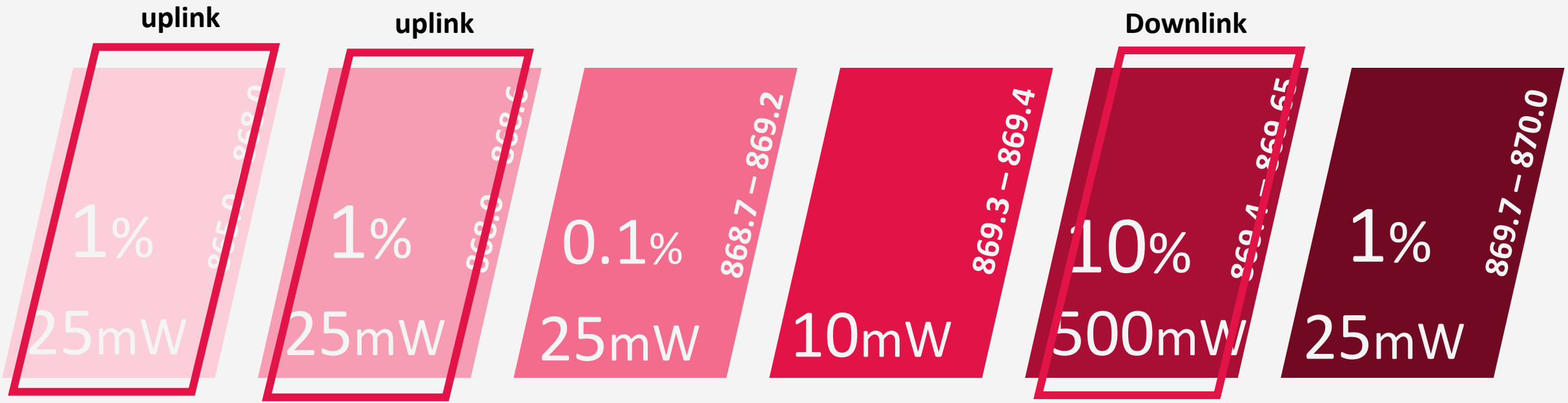
Defines the frequencies to be used (part of them), the frame format, encryption, ADR commands and the way to join a network

2 join procedures has been defined: OTAA (regular one, with session keys negotiation) and ABP (where the sessions keys are static). Over The Air Activation vs Activation By Personalization.

Defines the encryption procedures

Encryption is mandatory in a system where multiple networks co-exist. The encryption protects each operators against the competition as it protects the customer payload to be captured. The algorithm and the key generation are defined by the LoRaWAN specifications.

USE OF 865Mhz-870 Hz



LoRaWAN defines, for Europe, 3 standard channels any device will use for the JOIN process. Each of them are 125kHz (375KHz are used). Center frequency are 868.1 868.3 and 868.5 in Europe. They are occupying all the 868.0 -> 868.6 band. LoRaWAN networks in Europe supports 8 channels, other 5 channels are defined by the network operator, usually, in the other 1% bands.

In FCC zone, the constraint is to use a minimum of 64 different channel with channel hopping. This requires 64 LoRaWan gateways (rare and expensive) most of the implementations currently implement only 8 channels gateways. The devices will have to communicate over 64 channels to respect the regulation. Consequently, 75% of communications are lost.

LoRaWAN 3 communication classes

A Class – uplink and downlinks right after an uplink

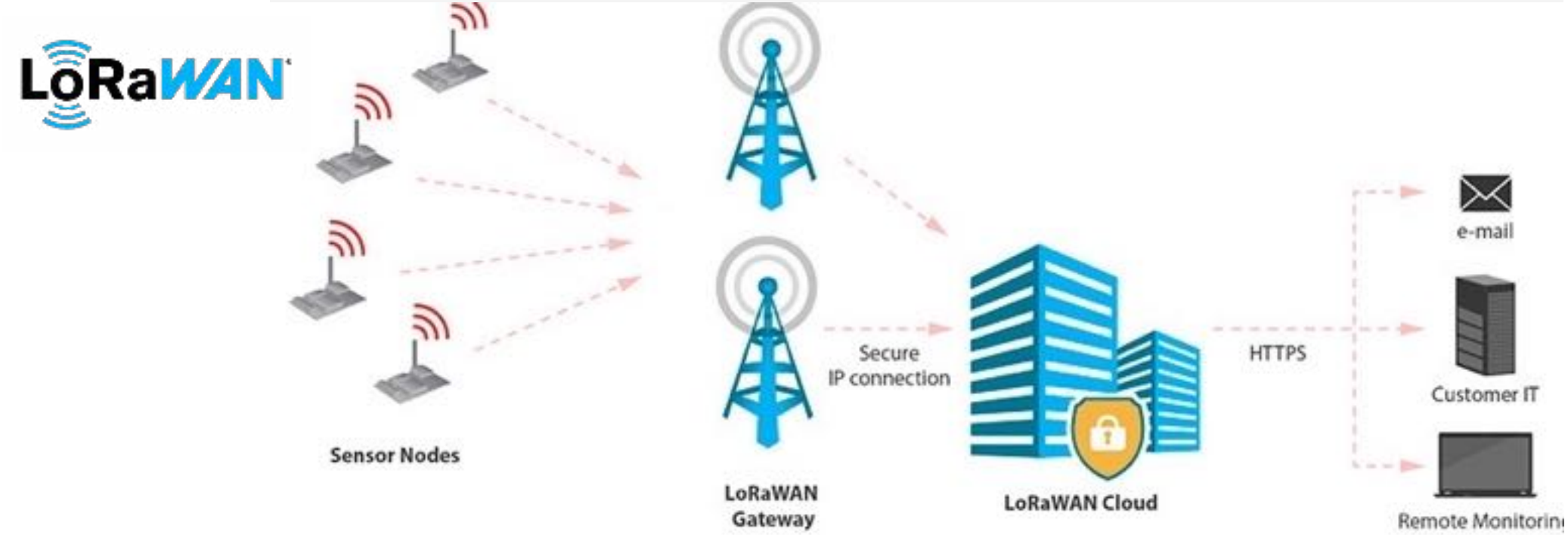
One of the available, non busy, channel is selected for the transmission. Once the communication has been made, the selected channel is busy according to the regulation. This communication can be followed by a downlink response when the device request for it. This downlink can have a payload or simply be an acknowledgement from the network. Gateway downlink capability is limited.

B Class – scheduled downlink

Instead of having to transmit a data to be able to receive a message, this mode allow to have a rendez-vous. It means clock synchronization and it is rarely implemented but allows multicast like for firmware distribution.

C Class – continuous reception

This is basically a Gateway mode. It is applicable for powered components as reception is power consuming (even if less than transmission)



LoRaWAN architecture

All the DEVICES are communicating to GATEWAYS, a gateway receives all the LoRaWAN messages, this includes messages already received by another gateway of the network. It also includes GATEWAY from other networks. All the packets are transferred to the NETWORK SERVER (LoRaWAN cloud here)

The NETWORK SERVER is decrypting the communication (only the NETWORK SERVER you belongs to have the keys for it), it also manage the JOIN procedure and ADR (Adaptative Data Rate) parameters with the DEVICES. It also forward the PAYLOAD to the CUSTOMER IT usually using HTTP POST or MQTT integration protocol.

Device identification

OTAA INPUTS

DevEUI

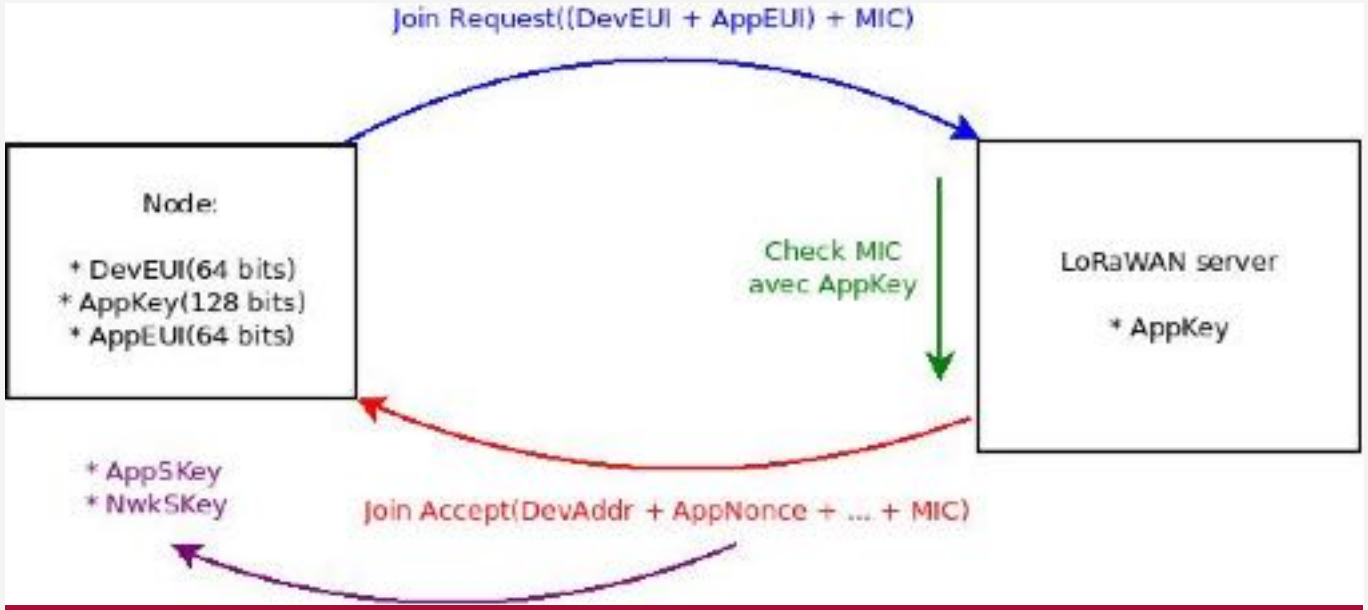
Device Uniq ID – IEEE unique (64b)

AppEUI

Application Uniq ID – IEEE unique (64b)

AppKey

Secret KEY only knows by the device and the Network Server. Used for generating signature and encryption keys. (128b)



OTAA OUTPUT

AppSKey

Session key used to encrypt the communications

NwkSKey

Session key used to sign the communications

DevAddr

Device ID to be use during the current session. This is a 32b ID, shorter than the DEV EUI.

FRAME FORMAT

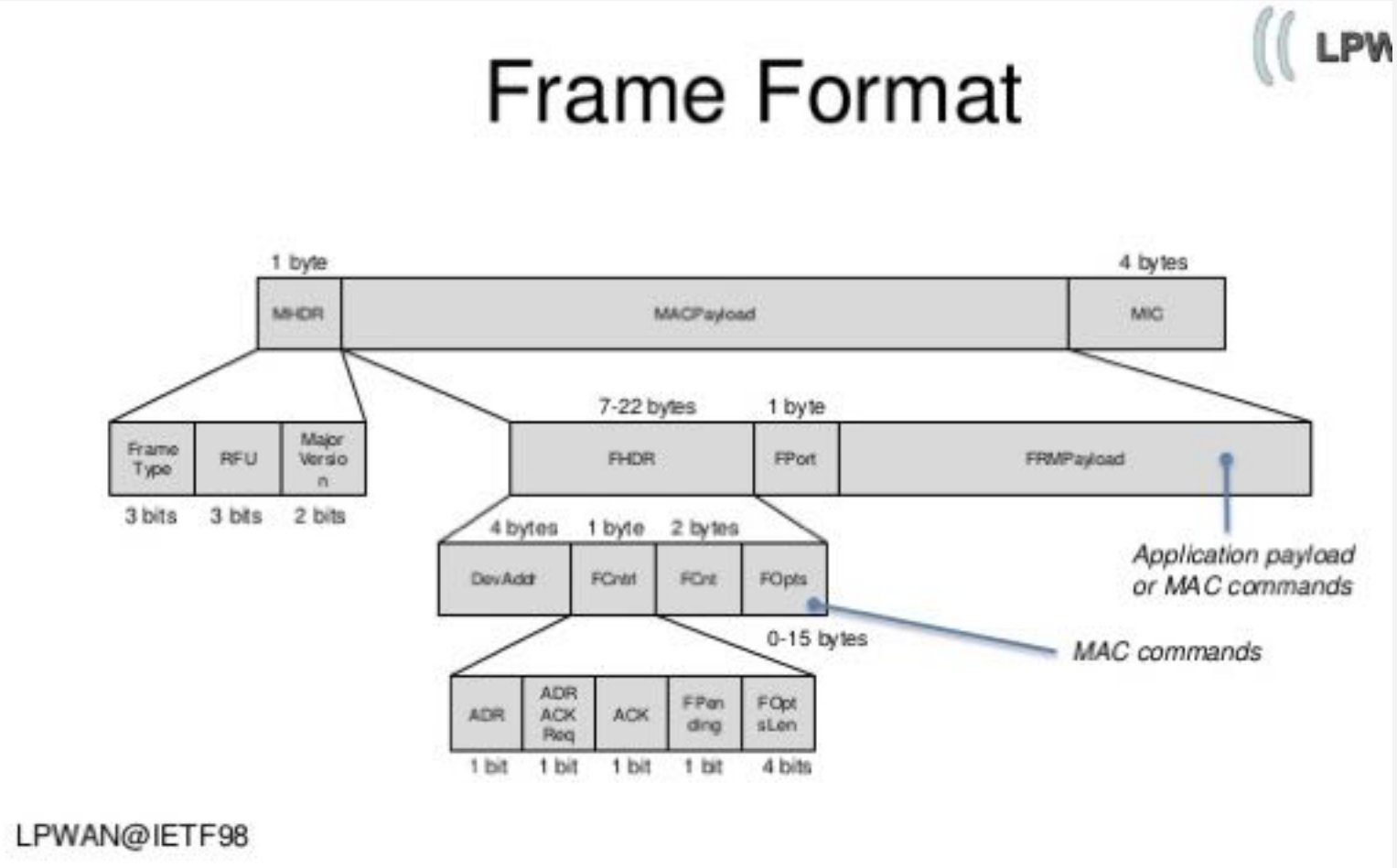
MAC Command

Allows the network server to place some specific request to the device like force a Spread Factor, channel list, transmission power …As a designed you must manage configuration change you did not expect.

MIC

Frame authentication

Protocol complexity is higher than Sigfox, therefore, the memory and flash footprint for LoRaWan is higher than Sigfox. For this reason ultra-low-cost is not a reachable target for it.



LoRaWAN DOWNLINKS

DOWNLINK are immediately following an UPLINK communication

The first one is on the same frequency as the UPLINK 1 second after it

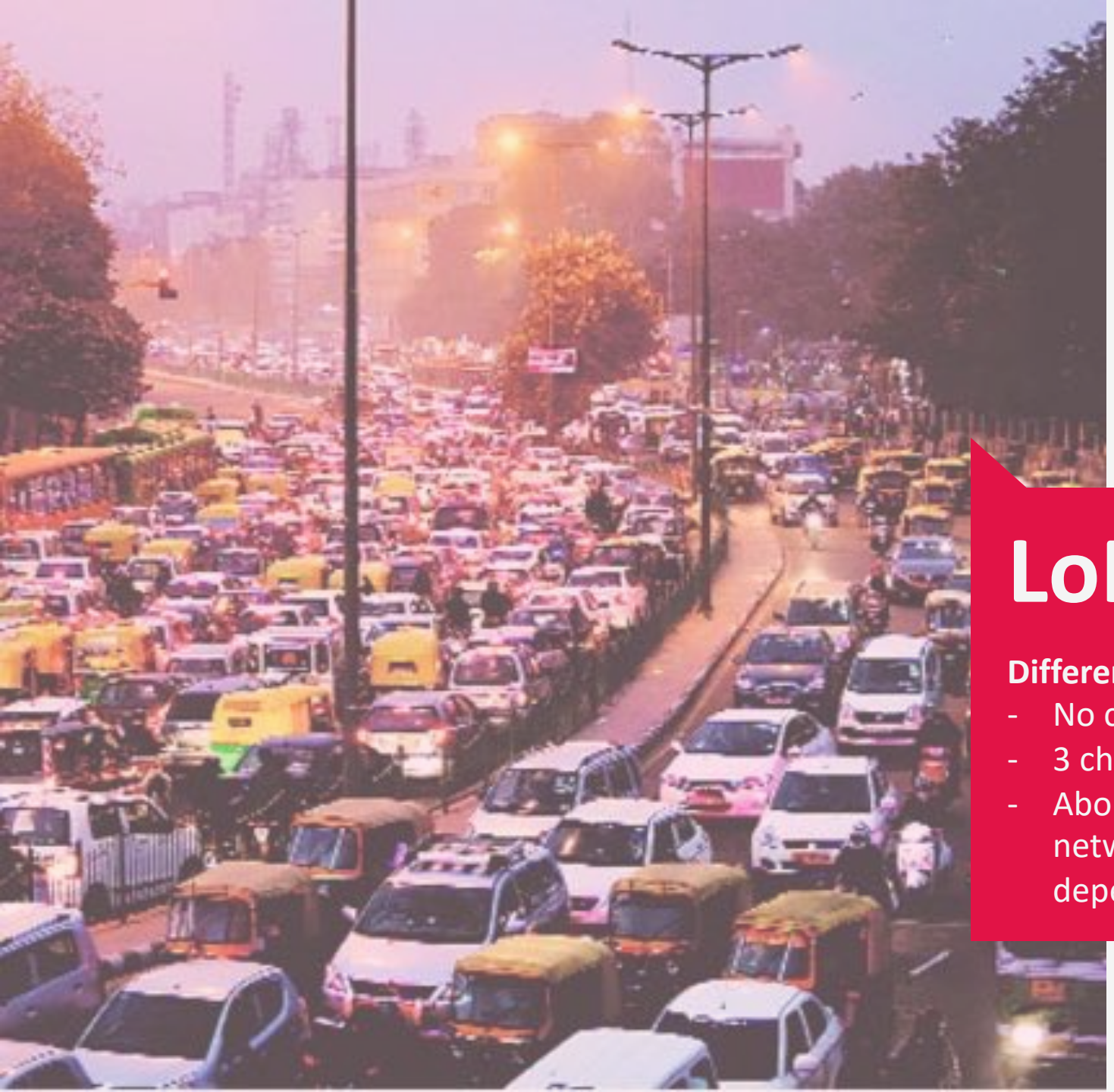
Speed can be different. The channel rules are applied (power, duty-cycle…)
This time is short for a Gateway – Network Server communication.

The second one is on 869.525Mhz allowing a 27dBm transmission

It happen 2 seconds after Uplink. Gateway gets more time to receive the Payload from the Network server

A downlink is acked by the device, multiple downlinks can be chained.

The downlink payload have to be queued in the network server: there is not enough time to loop the request with the customer IT.



LoRaWAN scalability

Different factors are limiting the scalability

- No congestion management
- 3 channels are common for all the networks
- About 1000 device in a same area (even in different networks) will saturate the 8 available channels. (it depends on SF and duty cycle…)

LoRaWAN STRENGHT AND WEAKNESS

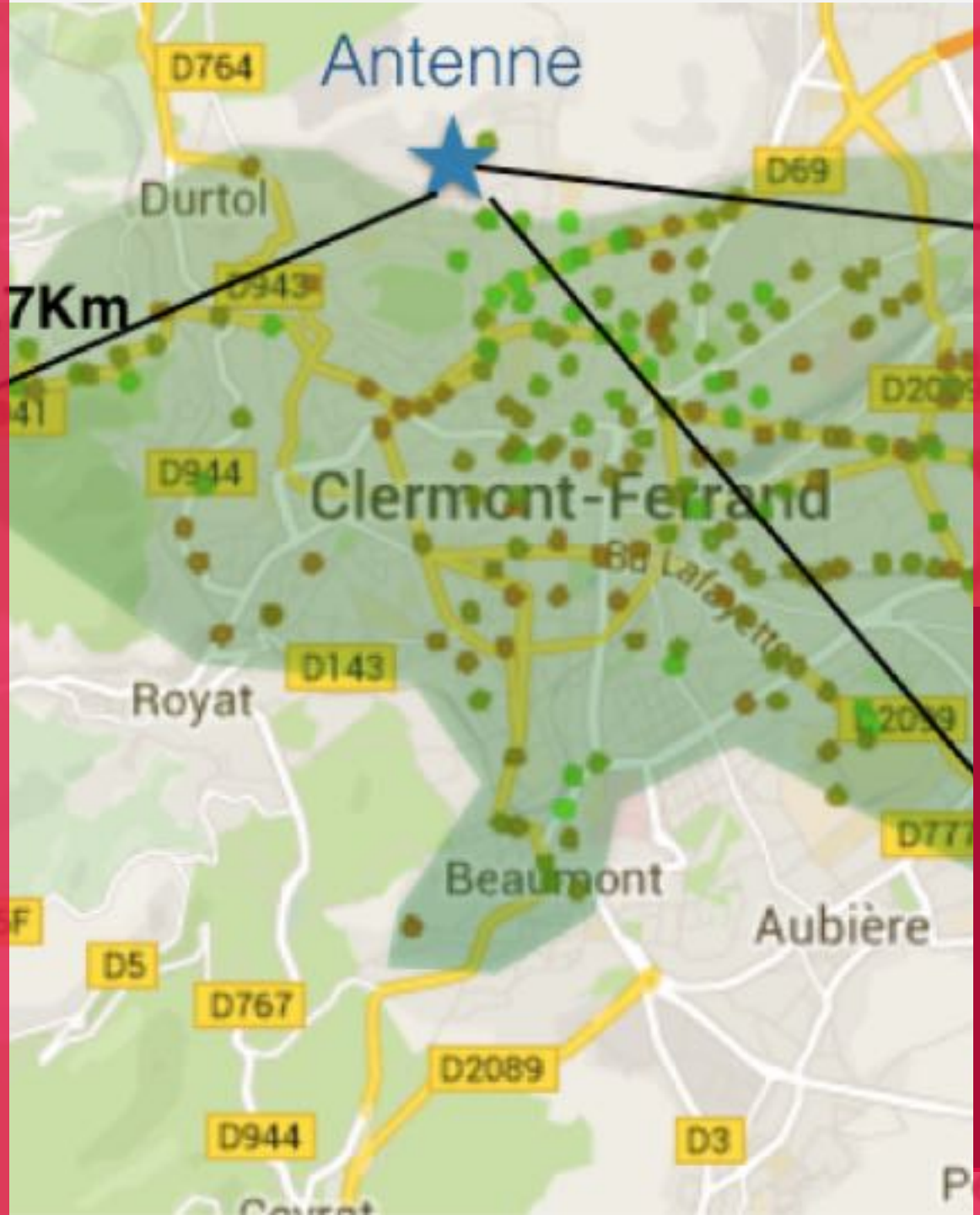
Strength

- Ability to offer TDOA location computing (Time Difference Over the Air) for non-GPS tracking (hundreds of meter precision)
- Ability to deploy private networks at low cost.
- Ability to support mobility with a reasonable loss rate.
- Throughput enabling multiple use-cases.

Weakness

- Complex channel management in roaming and complex roaming. Channel map for a network operator have to be global.
- A really limited number of public offer and complex roaming capability makes it limited to private usage or country usage when covered.
- Software complexity making it a bit more expensive than competitors on the device side. Even if the price is decreasing. Today it is starting at 5€ / device.

Private deployments



Public Application

The map displayed here has been made with a single LoRaWan antenna network deployed in a high position. All the city around is covered. The investment is about 500€ in 2020 for a such result.

Smart city application

Sensors deployed all around the city

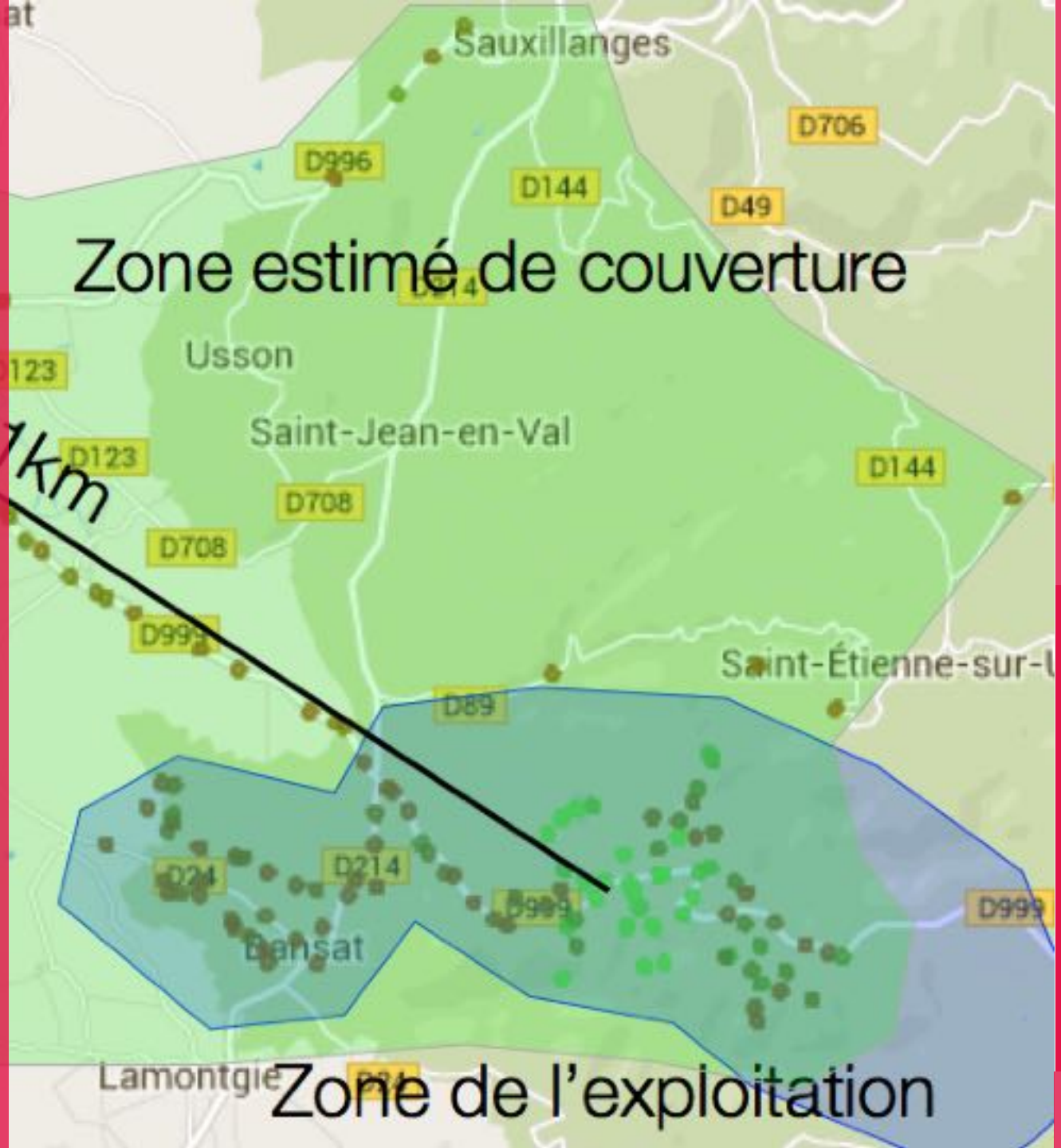
Local mobility

Collect information about public transport or parking availability …

Public network

Offering an IoT network access to all the citizens for private purpose.

Private deployments



Industrial Applications

Many industrial sector can get benefit of low-cost wide area networks.

This map has been made with a gateway on top of an Agricultural building. It basically cover all the area where the farmers are working and much more.

Agricultural domain

Get sensors data from field, animals, machines in real time.

Mining

Usage, performance, maintenance, vehicule tracking, people safety … Many application in area where classical network access is limited.

Industry

Provide a global coverage on an industrial site, process reporting, safety, inventory management…

Private deployments

What we get with a simple indoor gateway

An investment around 300€ allows to get a coverage in an industrial site, even Indoor and without interacting with existing network

Indoor vs Outdoor coverage

10 km coverage is what you can get with a good outdoor spot.
Indoor antenna performance are usually around 300m around.

On the left: an example of two gateways coverage (outdoor has a larger coverage than what your see here, outdoor did not).
Scale is the same

The Things Network

Is a crowdsourced network, deployed World-wide and free for use. Deployed by passioned people it proposes a good quality network In the main big cities.

Open-source mindset. This network is use in many business application: the network server is use for simplifying private deployment.

A professional version is available with Network Server SLA. TheThingsIndustry is the most innovative organization in the LoRaWan area since 2015. They are also pushing the market by making low-cost hardware and opensource solution.

Basically it is Uber for Telecom industry

Crowdsourced

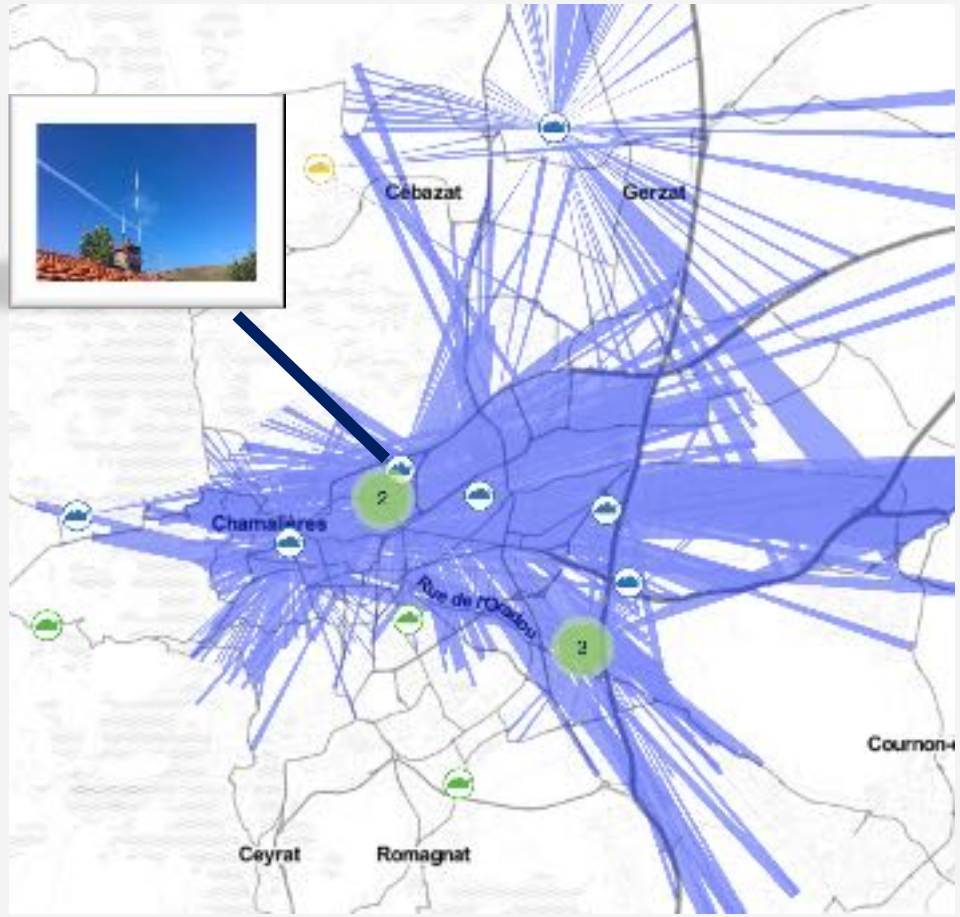
Created in 2015

15900 Gateway running
In 150 countries
500.000 devices using it

Most of the gateways have been deployed in Europe.

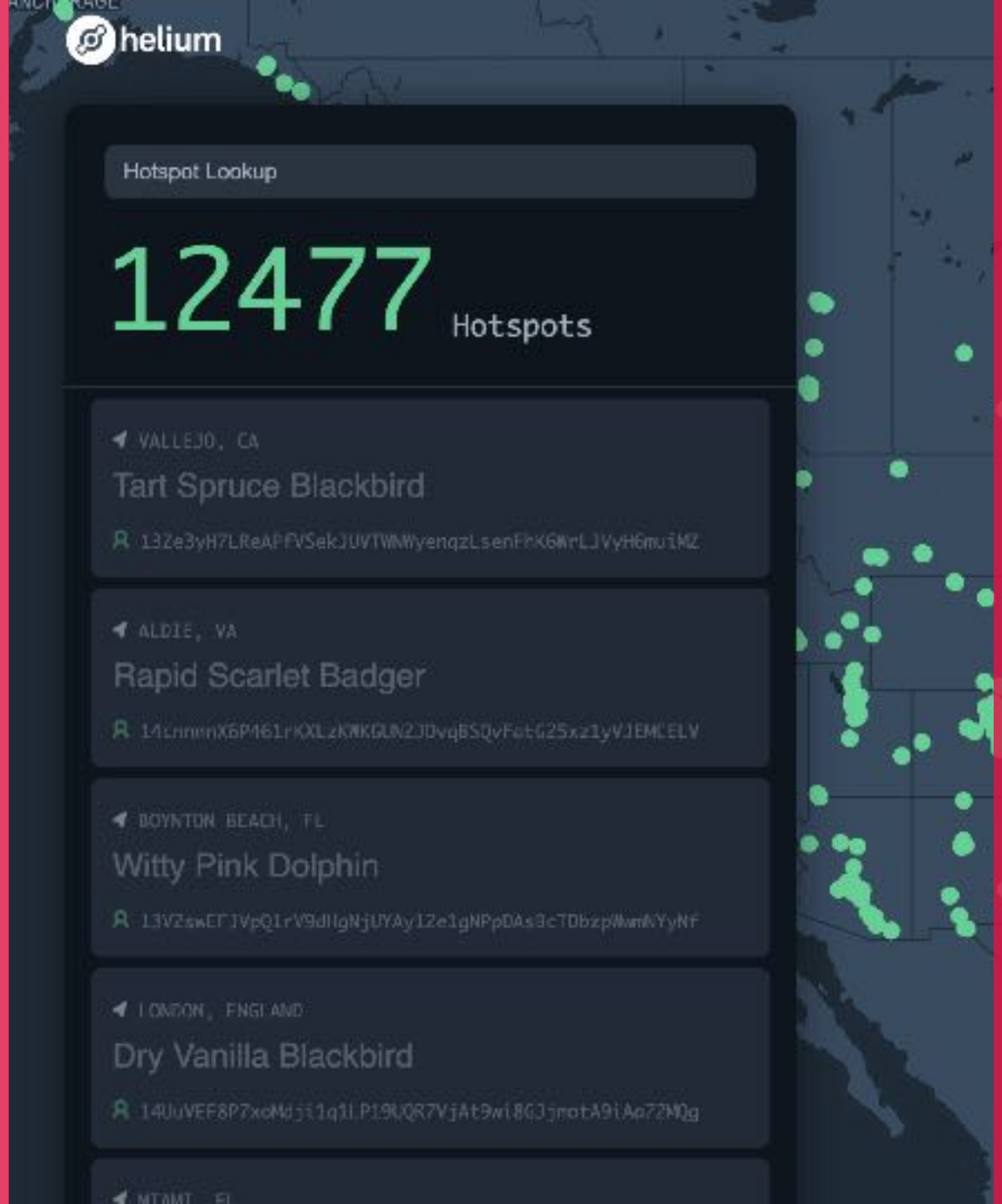
Crowdsourced

THE THINGS NETWORK



Coverage example made by a short number of people in a medium size city.

Crowdsourced



HELIUM

Is also crowdsourced IoT network, but it targets a different category of people to deploy the network. Instead of tech passionate, it target crypto investors.

Helium is an IoT network managed with a blockchain. Helium contributor are mining HNT tokens against coverage.
Communication are billable with a flat and low price.

Basically it is UBER + BITCOIN for Telecom industry

Crowdsourced

12500 Hotspot deployed in 6 months. Mostly in the USA.

Growing fast as today your cash back is about 2 weeks.

Limited coverage due to indoor installation in most of the cases.

3GPP - Traditional telecom technologies applied on IoT

Multiple technologies

LTE-M is a power saving version of LTE (aka 4G)
NB-IoT is the LPWAN solution from 3GPP
Both have been added in best effort mode to 4G

Both will natively be provided and improved with 5G equipment's.

Telecom operator technologies

- LTE-M => LTE-MTC - Machine Type Communication
- eMTC => enhanced Machine Type Communication
- LTE CAT-M1/2

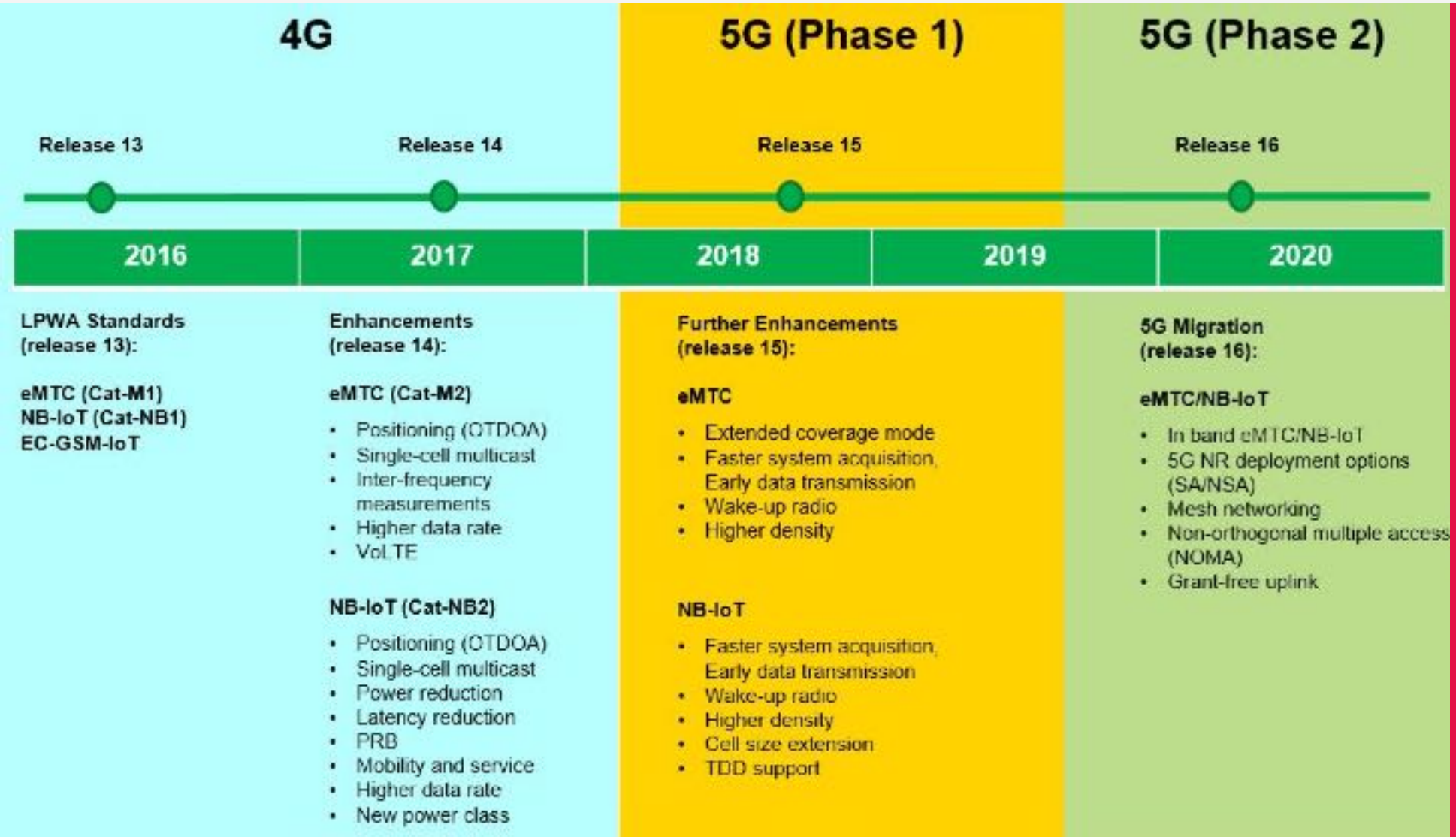
- IP Based – directly accessible

- LTE CAT-NB1/2 => Narrow Band
- Accessible through an operator network kernel

Both are using licensed spectrum with no duty-cycle restrictions

Both are deployed by telecom operator and subject to subscription

3GPP Roadmaps



LTE-M is
- Cat-M1/Cat-M2
- eMTC

Nb-Iot is
- Cat-NB1/Cat-NB2

Release 13 has been deployed in France in 2019 for LTE-M (Orange)

Release 13 has been announced in France in 2019 for Nb-IoT (SFR)

Deployment time-line is impacted by chip time-to-market

Radio chips are available 18 month after spec

The chip industry need a reasonable time to implement the new 3GPP specification in silicon. It's about 18 months process before getting a released version. Then the design of object hardware can start for a second 18 months process. Therefore we have a 3 years shift between technology announcement and market availability.

On the operator side update can be software when the within the same generation. Hardware deployment (with large investment) is needed to change from a generation to the next one.

3GPP Solutions

LTE-Cat M / LTE-Cat NB are solutions based on 4G (LTE)

V·T·E [7][8]	LTE Cat 1	LTE-M				NB-IoT		EC-GSM-IoT
		LC-LTE/MTCe	eMTC					
		LTE Cat 0	LTE Cat M1	LTE Cat M2	non-BL	LTE Cat NB1	LTE Cat NB2	
3GPP Release	Release 8	Release 12	Release 13	Release 14	Release 14	Release 13	Release 14	Release 13
Downlink Peak Rate	10 Mbit/s	1 Mbit/s	1 Mbit/s	4 Mbit/s		27 kbit/s	80 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Uplink Peak Rate	5 Mbit/s	1 Mbit/s	1 Mbit/s	7 Mbit/s		62 kbit/s (multi-tone) 20 kbit/s (single-tone)	105 kbit/s	474 kbit/s (EDGE) 2 Mbit/s (EGPRS2B)
Latency	50–100ms	not deployed	10ms–15ms			1.6s–10s		700ms–2s
Number of Antennas	2	1	1			1		1–2
Duplex Mode	Full Duplex	Full or Half Duplex	Full or Half Duplex			Half Duplex		Half Duplex
Device Receive Bandwidth	1.4 – 20 MHz	1.4 – 20 MHz	1.4 MHz	4x1.4 MHz		180 kHz	180 kHz	200 kHz
Receiver Chains	2 (MIMO)	1 (SISO)	1 (SISO)			1 (SISO)		1–2
Device Transmit Power	23 dBm	23 dBm	20 / 23 dBm			20 / 23 dBm		23 / 33 dBm

At least a software update is needed on all operator equipments over 4G.

3GPP Solutions in the 5G

	Next Generation
	5G
Range (Outdoor)	< 15 km
MCL	164 dB
Spectrum	Licensed (7-900 MHz)
Bandwidth	shared
Data Rate	<1 Mbps
Battery Life	>10 years
Availability	2025

5G release 15 is still not really documented on Internet about LTE-M & NB-IoT improvement.

Operators need to change all the telecom equipment to support 5G.

LTE-M outdoor coverage

Orange network coverage in France. Dark orange is indoor coverage. Light orange = outdoor only.

Basically 4G network coverage