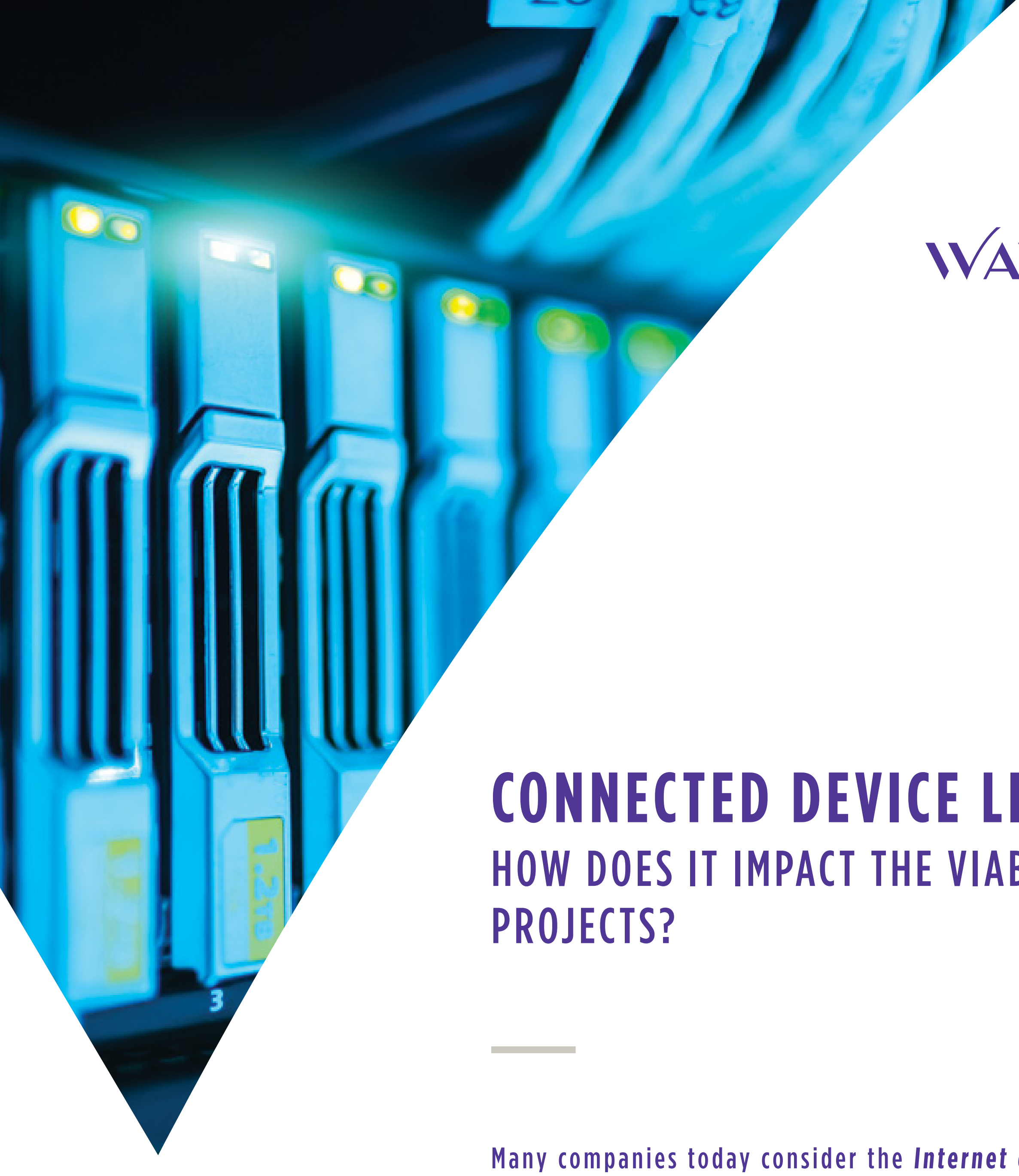
The Positive Way
WAVESTONE



CONNECTED DEVICE LIFE CYCLE:

HOW DOES IT IMPACT THE VIABILITY OF IOT PROJECTS?

Many companies today consider the ***Internet of Things*** (IoT) to be a new method of transforming their business, creating service offerings, increasing operational performance, or responding to new regulations. However, industrialization and the increasing scale of IoT projects, which may involve millions of connected devices, make it necessary to prepare for the management of the connected devices' life cycle in order to ensure the longevity of implemented solutions. Maintaining operational and security aspects becomes increasingly complex as the volume and diversity of connected devices grows, as anything can happen when working with fleets that consist of millions of devices.

To successfully industrialize their IoT projects, companies need to ask themselves the right questions. What are the stages of their connected device life cycles? What impacts does this have on their IoT projects? Which teams are implicated? What is the level of integration with the existing IS and more broadly with the project environment? This publication aims to provide the answers to enable successful IoT scaling.

CONTACTS

Alice MORIZE
alice.morize@wavestone.com

Romain POINTEREAU
romain.pointereau@wavestone.com

This publication was produced with the support of Maximilien Bouilly, Julia Franco, Taha-Mahmoud Gaidi, Maxime Gérard, Kévin Guerin and Benoit Tanguy.

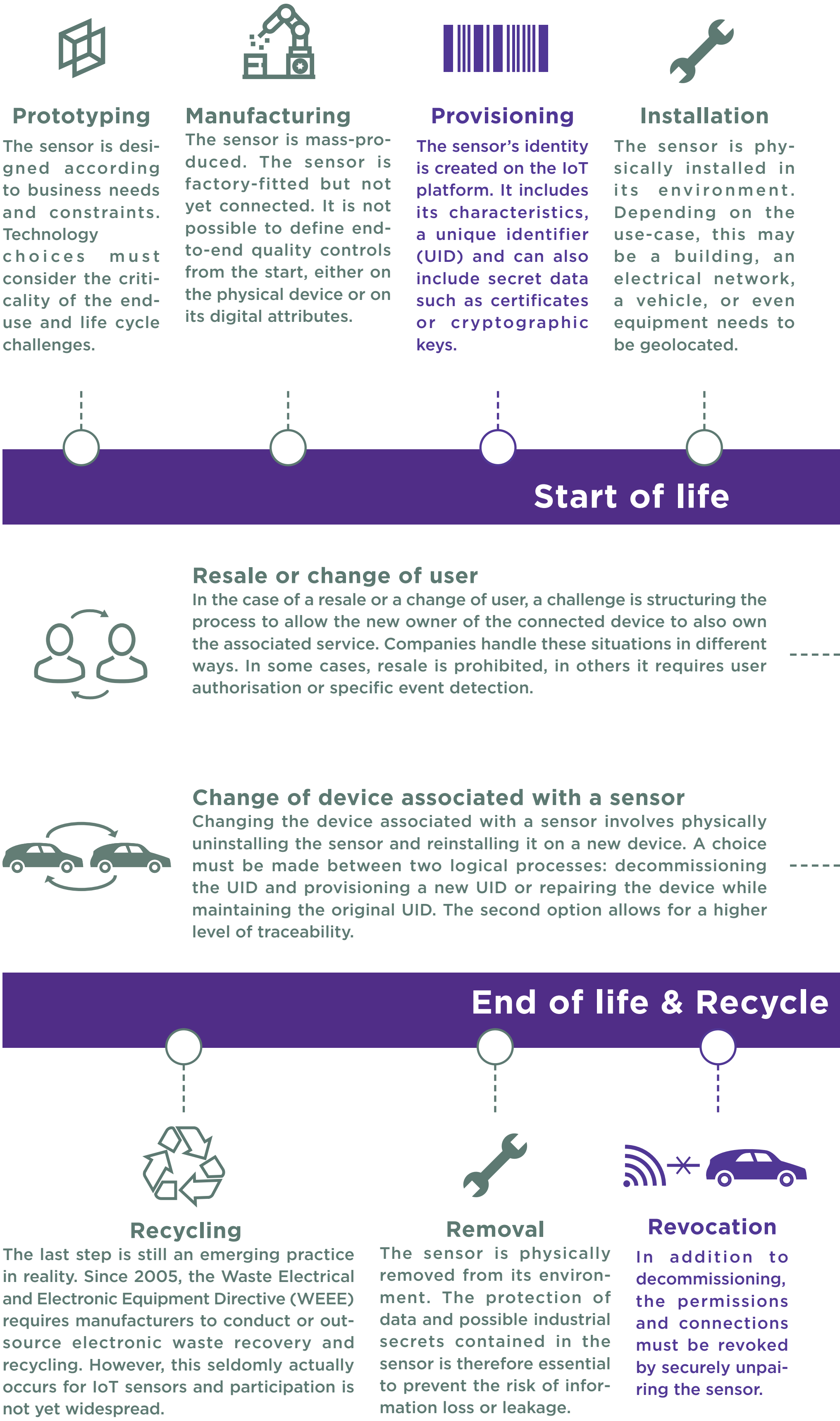
A few definitions

- A **sensor** is a measurement device that transmits captured data over a network. In this publication, the term sensor may refer to a single sensor, a system consisting of a gateway and several sensors, or a more complex system with *Edge Computing* capabilities.
- A device is connected when it is equipped with a communication sensor. A connected device therefore refers to the combination of the sensor and the associated equipment or environment.
- The **IoT** is a system of connected devices that can communicate with an IoT platform[1].

CONNECTED DEVICES: A LIFE CYCLE PUNCTUATED BY SEVERAL STAGES

Different stages separate the life cycle of connected devices concerning both the physical connection of the connected device and the logical pathways of the information that characterises it. These stages should be fully estimated as early as the scoping phase of an IoT project to ensure that it is economically and operationally viable and that it is secure[2].

Typical life cycle stages for connected devices



Prototyping
The sensor is designed according to business needs and constraints. Technology choices must consider the criticality of the end-use and life cycle challenges.

Manufacturing
The sensor is mass-produced. The sensor is factory-fitted but not yet connected. It is not possible to define end-to-end quality controls from the start, either on the physical device or on its digital attributes.

Provisioning
The sensor's identity is created on the IoT platform. It includes its characteristics, a unique identifier (UID) and can also include secret data such as certificates or cryptographic keys.

Installation
The sensor is physically installed in its environment. Depending on the use-case, this may be a building, an electrical network, a vehicle, or even equipment needs to be geolocated.

Start of life

Resale or change of user
In the case of a resale or a change of user, a challenge is structuring the process to allow the new owner of the connected device to also own the associated service. Companies handle these situations in different ways. In some cases, resale is prohibited, in others it requires user authorisation or specific event detection.

Change of device associated with a sensor
Changing the device associated with a sensor involves physically uninstalling the sensor and reinstalling it on a new device. A choice must be made between two logical processes: decommissioning the UID and provisioning a new UID or repairing the device while maintaining the original UID. The second option allows for a higher level of traceability.

End of life & Recycle

Recycling
The last step is still an emerging practice in reality. Since 2005, the Waste Electrical and Electronic Equipment Directive (WEEE) requires manufacturers to conduct or outsource electronic waste recovery and recycling. However, this seldomly actually occurs for IoT sensors and participation is not yet widespread.

Removal
The sensor is physically removed from its environment. The protection of data and possible industrial secrets contained in the sensor is therefore essential to prevent the risk of information loss or leakage.

Revocation
In addition to decommissioning, the permissions and connections must be revoked by securely unpairing the sensor.

[1] IoT Platforms: the cornerstone of a successful IoT strategy: https://fr.wavestone.com/fr/insight/plateformes-iot-cle-de-voute-strategie-iot-reussie/

[2] A life cycle approach to IoT security: https://www.riskinsight-wavestone.com/2019/09/cycle-vie-securite-iot/

○ Steps associated with the physical connection of the connected device

○ Logical steps related to the information associated with the connected device

Pairing

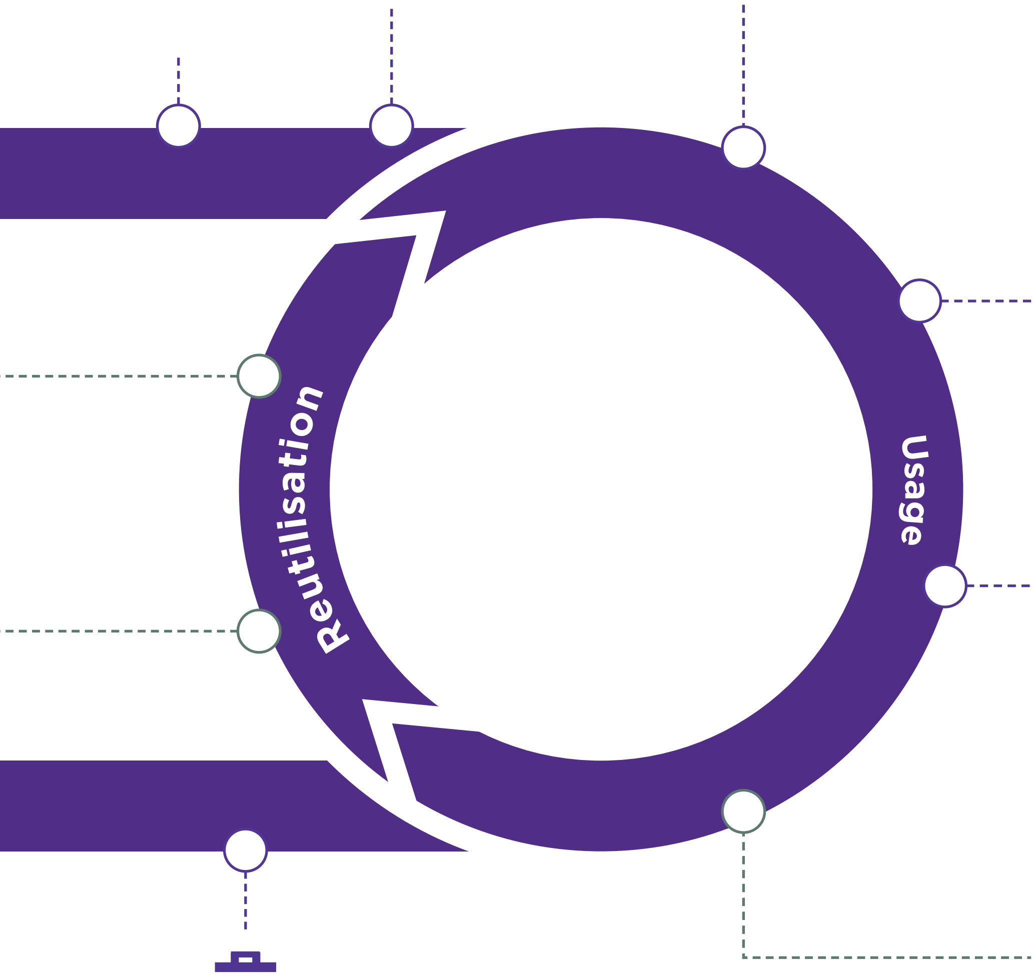
Pairing links a sensor with its associated device. This step verifies that a specific data stream comes from a specific device.

Enrolment

Registering a connected device on its IoT platform allows it to begin communicating. This is also necessary to ensure that the connected sensor is legitimate.

Monitoring

IoT platforms enable remote monitoring of connected devices, includes indicators such as operating status, battery level, configuration settings, or software version.



Alerts

Alerts are configured according to the risk events that you wish to detect, for example transmission of erroneous data.

Over-the-Air Updates

This feature, commonly known as OTA, allows the connected device to be remotely updated and configured wirelessly. It is an important and complex tool in the management of connected device's life cycle3.

Maintenance Operations

Detection of a sensor malfunction triggers a maintenance operation. This may involve a physical action, such as repairing or replacing a component, or a remote action, such as OTA recalibration of a sensor.

Decommissioning

This allows the secure removal of the connected device from its associated platform.

[3] This feature is detailed in the insert «The Expert's Eye on OTA» (pages 6 and 7).

ENVIRONMENT INTEGRATION: A DRIVER FOR SUCCESSFUL LIFE CYCLE MANAGEMENT

In addition to defining a connected device's life cycle, it is important to identify the key stakeholders. For example, the following participants play a significant role:

- **Sensor manufacturers** are the primary sensor information owners, such as their identity or properties;
- **Logistics teams** manage the sensor supply chain from procurement to dispatch to installation, and even to end-users.
- **Field teams** are responsible for the physical operations related to connected devices, including installation, maintenance or removal;
- **The teams in charge of the IoT plat-form** are normally in charge of technical procedures such as pairing of devices, provisioning of data or system updates.

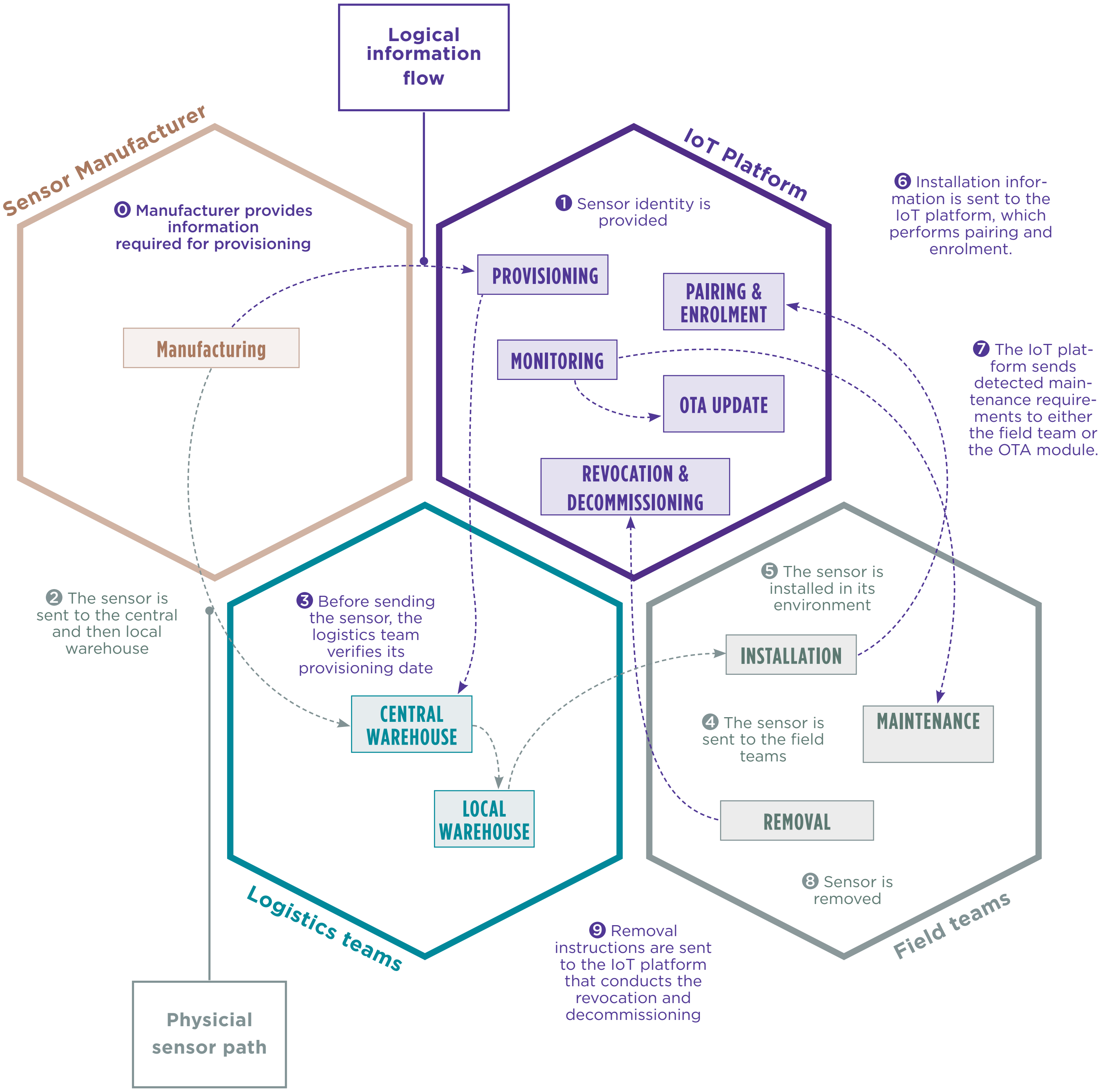
Therefore, it is important to consolidate all of the information held by these stakeholders in order to effectively manage the entire connected device life cycle.

It is essential to formally establish **the inputs and activities expected from each** of the stakeholders on the physical or logical life cycle stages.

As an example, a key process to secure is the synchronisation of the data received by the physical sensor with the data received by its digital twin. The obligations made for the delivery of digital data should be identical to those made for physical delivery. This also applies for support and maintenance.

A possible distribution model is shown on the next page.

Inputs of each team throughout the connected device life cycle


Logical information flow
Sensor Manufacturer
⓿ Manufacturer provides information required for provisioning
Manufacturing
IoT Platform
❶ Sensor identity is provided
PROVISIONING
PAIRING & ENROLMENT
MONITORING
OTA UPDATE
REVOCATION & DECOMMISSIONING
❻ Installation information is sent to the IoT platform, which performs pairing and enrolment.
❼ The IoT platform sends detected maintenance requirements to either the field team or the OTA module.
❷ The sensor is sent to the central and then local warehouse
❸ Before sending the sensor, the logistics team verifies its provisioning date
CENTRAL WAREHOUSE
LOCAL WAREHOUSE
Logistics teams
❺ The sensor is installed in its environment
INSTALLATION
❹ The sensor is sent to the field teams
MAINTENANCE
REMOVAL
❽ Sensor is removed
Field teams
❾ Removal instructions are sent to the IoT platform that conducts the revocation and decommissioning
Physicial sensor path

Once the inputs have been properly defined, integration between the various team environments is necessary.

As the teams involved may evolve over time, for example if there is a change of supplier or a scope change, it is necessary to adopt **a standard way of integrating new components**. An evolutionary architecture must be designed through the implementation of a modular architecture composed of standalone micro-services, the presentation of services through APIs, or by using open protocols.

Simultaneously, to ensure data integrity, it is recommended to create **a single repository of connected devices with their associated status.** This repository should be updated by the both the business and by each of the teams mentioned above. This repository can be composed of one or multiple databases, however the access portal must be unique. The appointment of a repository manager for the connected devices is required to ensure overall data integrity.

Finally, some companies choose to **store all or a portion of their status logs to capture the full lifecycle of each connected device.** Whether or not this practice improves traceability, the benefits must be assessed on a case-by-case basis depending on the relevance of the information and the associated timeframe.

EXPERT VIEW ON *OVER-THE-AIR UPDATES* (OTA)

OTA allows various actions to be performed remotely on a connected device and can be divided into three categories. From the most basic to the most complex these are:

/ **COTA** *(Configuration Over-The-Air)* allows you to change the connected device's settings, such as connection frequency or default settings;

/ **SOTA** (*Software upgrade Over The Air*) allows you to update the connected device's software and applications;

/ **FOTA** (*Firmware upgrade Over The Air*) allows you to update the connected device's operating system.

OTA offers benefits at several levels

There can be a significant lead time between the production of a sensor and its usage. Therefore, it is recommended to use OTA to **keep software updated** in order to avoid additional preparation before putting a sensor into service. This flexibility allows large orders to be placed at once facilitating scalability.

OTA also makes it possible to **fix software defects in connected devices** that have already been deployed, avoiding costly alternatives such as mass recall or manual maintenance by a technician.

Additionally, many connected devices have cyber security vulnerabilities embedded in their software, such as weak passwords or unencrypted data. The risk exposure is therefore considerable for companies looking to scale their operations. The integration of SOTA or FOTA capabilities at the connected device's design stage is an important consideration in order to **maintain a secure environment.**

Finally, a **significant reduction in *time-to-market*** is made possible by OTA. In this case, OTA updates are used to improve a connected device's software features in the future.

Nevertheless, OTA is a complex process that raises a number of unique challenges

The first challenge when it comes to OTA is the update process. In order to avoid the need to support a wide range of sensors with different versions, and to increase the level of security, **an automatic update policy** can be considered to keep devices on the latest software version. However, this policy requires frequent updates at a large scale. Therefore, it is necessary to design an adequate OTA infrastructure and to bear these associated costs.

Physical limitations related to *hardware* must also be accounted for. For example, since RAM or CPU memory is limited, the sensor should be designed to be upgraded in the future.

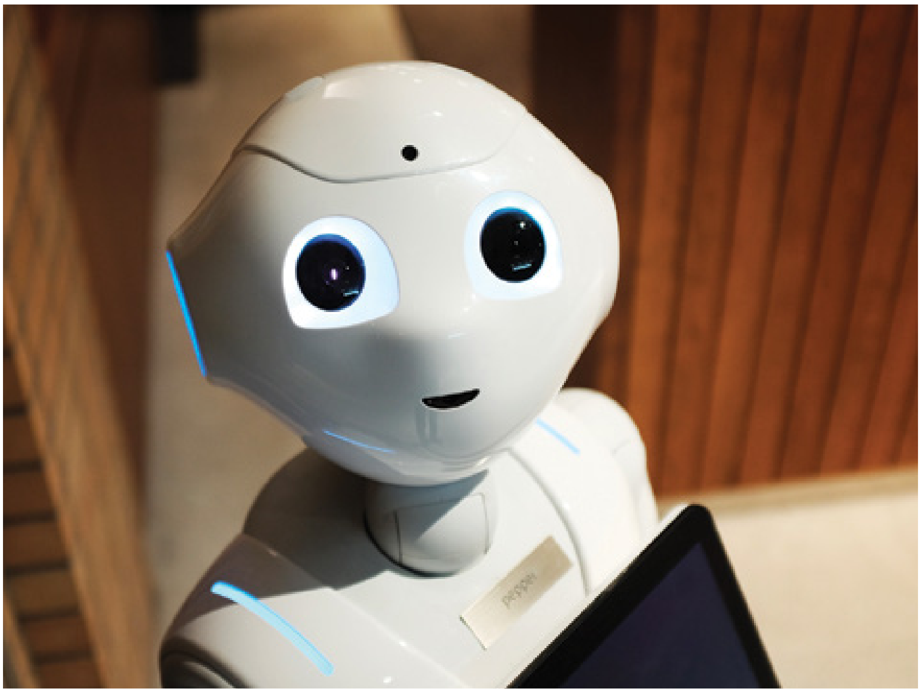
Choosing the right OTA platform is also crucial. It can be distinct from the IoT platform. It should be selected by ensuring its compatibility with existing IS, connected devices and the IoT platform where applicable.

Additionally, depending on the use case, an **incremental or full update** may be used. While incremental updates are faster and cheaper due to their smaller size, they are also more complex to install when multiple software versions are actively used across the device pool. Alternatively, full updates can increase the risk of malfunction if the previous software version is deleted when the new version is installed.

Choosing the appropriate time to apply updates should also be considered in relation to the specific use-case and the resulting impact from a service interruption. Updates can be initiated when the device is turned off, as with connected vehicles and PCs, or it can be started manually, such as for smartphones.

Finally, the **connection between the OTA platform and the connected device** must be secured end-to-end to prevent man-in-the-middle attacks, DoS, DDoS, or malicious code injection.

Hence, the **update process must be particularly scrutinised** from the start of an IoT project in order to ensure no vulnerabilities are introduced.



In general, the success rate of OTA is highly dependent on anticipating individual cases based on specific scenarios; however, it is still ideal to anticipate all possible scenarios. **OTA does not preclude the need for on-site remediation.** Indeed, these two activities must be done in conjunction with one another. This means investing in a robust OTA solution that can cover as many scenarios as possible while also ensuring that local access to sensors is secure. The return on investment will then come from reduced operational and security maintenance costs.

In the market, specific OTA solution providers stand out from the crowd

By analysing the IoT systems deployed by major companies, it is evident that COTA functionalities are often executed by an IoT platform while the more complex SOTA and FOTA functionalities are executed by dedicated OTA platforms provided by specialised players.

Thus, **the major COTA suppliers continue to be the large IoT platform** vendors that are normally used by major corporations, such as Azure IoT or AWS IoT, making COTA solutions relatively standardized across the market.

In contrast, **it is the niche players who supply most of the SOTA and FOTA solutions.** These solutions are generally more complex to implement because they depend on the specific connected device that is used. Generally, this requires installing a specific agent on the connected device which manages software and firmware installations as well as the communication between the platform and device. This strong dependence on the embedded solution explains how vertical and niche players differentiate themselves from the competition. These include Airbiquity and Uptane, who specialise in the automotive sector, the manufacturer Bosch, mobile software management provider Red Bend and open source solution providers hawkBit and Mender. The dependency of the connected device on the OTA platform impacts the ability to switch from the chosen platform in the future.

CONCLUSION

Thus, each stage of the connected device life cycle influences the viability of IoT solutions. It is therefore essential to anticipate the entire cycle from the scoping phase by working closely with sensor manufacturers to ensure that all challenges are considered during the design process.

To guarantee the success of this overall management, using shared repositories, defining a governance framework and selecting open and scalable information system integration methods should be prioritised.

Success is also highly dependent on collaboration between the business lines and the CIOs as early as possible. This prevents IoT projects from being delayed when trying to scale-up by capacity of the IT teams. Companies must define IoT operating models adapted to their business objectives.

OTA illustrates how technological solutions can improve the life cycle management for connected devices. OTA offers a significant benefit in terms of maintaining security and operations, as updates can be made in an automated and scheduled manner.

Failure to treat OTA as a prerequisite for the validation of a scaleable IoT implementation would be a mistake.

There are other technological solutions, such as Digital Twins, which promise to facilitate the more complex aspects of large-scale life cycle management, such as simulations during sensors prototyping or predictive maintenance. In the coming years, these subjects will be at the core of IoT project implementation.

The Positive Way

WAVESTONE

www.wavestone.com

In a world where knowing how to transform is the key to success, Wavestone's mission is to enlighten and guide large companies and organizations in their most critical transformations with the ambition of making them positive for all stakeholders. This is what we call «The Positive Way».

Wavestone has 3,000 employees in 8 countries. He is one of the leading independent board members

in Europe, and is the leading independent consulting firm in France. Wavestone is listed on Euronext in Paris and has the Great Place To Work® label.

®.