NEXT GENERATION INTERNET

Grant Agreement No.: 957216
Call: H2020-ICT-2018-2020

Topic: ICT-56-2020
Type of action: RIA

D2.5 Advanced Business Models for IoT Services

Revision: v1.0

Work package	WP2
Task	T2.3
Due date	28/02/2023
Submission date	28/02/2023
Deliverable lead	Fivecomm (5CMM)
Version	v1.0
Editors	Manuel Fuentes (5CMM), Miguel Cantero (5CMM)
Authors	Manuel Fuentes (5CMM), Miguel Cantero (5CMM), Jose Costa-Requena (CMC), Joan Meseguer (FVP), César Rodríguez (TID), Efstathios Katranaras (SEQ), Nuria Molner (UPV), Jussi Poikonen (AWA), David Martín-Sacristán (5CMM), Clemens Saur (NCG), Christos Politis (SES)
Reviewers	Nicola Ciulli (NXW), Erin Seder (NXW), Nuria Molner (UPV), Irene Alepuz (UPV)

Abstract	The following document, D2.5, is the second deliverable of Task 2.3 and the last deliverable of WP2. The document first describes the iNGENIOUS ecosystem, that is, the different actors involved in the project and their role

	in the end-to-end IoT chain. Later on, the document focuses on an advanced business analysis of the IoT solutions for verticals. The objective of this document is to provide a wider overview of the market and complete the information provided in D2.3. Specifically, it provides an analysis on the business vision of vertical stakeholders (consortium members, AB, and external NG-IoT projects), and also by the IoT solution providers that are part of the iNGENIOUS consortium. Such vision has been obtained through two different questionnaires containing a wide variety of topics related to IoT and its ecosystem. The main idea is to compare both views and understand if our consortium is aligned with the stakeholders' perspective and the maturity of our portfolio is enough for the services expected.
Keywords	IoT, business analysis, vertical stakeholders, solution providers, SWOT, ecosystem, innovation

Document Revision History

Version	Date	Description of change	List of contributors
v1.0	28/02/2023	EC version	Manuel Fuentes (5CMM), Miguel Cantero (5CMM)

Disclaimer

Copyright notice

Project co-funded by the European Commission in the H2020 Programme		
Nature of the deliverable:	**R**	
Dissemination Level		
PU	Public, fully open, e.g. web	✓
CL	Classified, information as referred to in Commission Decision 2001/844/EC	
CO	Confidential to iNGENIOUS project and Commission Services	

** R: Document, report (excluding the periodic and final reports)*

DEM: Demonstrator, pilot, prototype, plan designs

DEC: Websites, patents filing, press & media actions, videos, etc.

OTHER: Software, technical diagram, etc.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Executive Summary

The following document, **D2.5**, entitled *Enhanced Business Models for IoT services,* is the second deliverable of Task 2.3, which covers the regulatory framework and business models of the iNGENIOUS project.

In particular, the deliverable is divided into two main parts. The first part provides details about the **iNGENIOUS ecosystem**, that is, the different actors involved in the project and their role in the end-to-end IoT chain. The identified key players are spectrum regulators, infrastructure owners, IoT technology solution providers, vertical stakeholders, and academia. This first overview will serve us to understand the context of the project and position the reader to better understand the following sections.

The second part of D2.5 focuses on an **advanced business analysis** of the IoT solutions for verticals. The objective of this part is to provide a wider overview of the market and complete the information provided in D2.3. Specifically, it provides an analysis on the business vision of the two main players of our ecosystem, i.e., vertical **stakeholders** and **IoT solution providers** that are part of the iNGENIOUS consortium. Such vision has been obtained through two different questionnaires containing a wide variety of topics related to IoT and its ecosystem.

The first questionnaire addressed vertical stakeholders, it was sent and answered by members of the iNGENIOUS consortium, Advisory Board members, and external industrial companies from **all RIA NG-IoT projects**, that is, Intell-IoT, VEDLIoT, TERMINET, IoT-NGIN, and ASSIST-IoT. Regarding the second questionnaire, it has been addressed to and answered by all partners with an exploitation element that has gone or will eventually go to the market as a product.

The main objective is to compare both views and understand if our consortium is aligned with the stakeholders' perspective and the maturity of our portfolio is in line with the services expected. The document also provides an extensive **SWOT analysis** from the perspective of the industry as well as per product offered by iNGENIOUS.

Co-funded by the Horizon 2020
Framework Programme of the European Union

Table of Contents

Co-funded by the Horizon 2020 Framework Programme of the European Union

List of Figures

Co-funded by the Horizon 2020 Framework Programme of the European Union

List of Tables

Co-funded by the Horizon 2020 Framework Programme of the European Union

Abbreviations

3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
5GC	5G Core
5GLAN	5G Local Area Network
AGV	Automatic Guided Vehicle
AI	Artificial Intelligence
BLE	Bluetooth Low-Energy
CAPEX	Capital Expenditure
CAT-M1	Category M1
DLT	Distributed Ledger Technology
E2E	End-to-end
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GW	Gateway
IIoT	Industrial IoT
IoT	Internet of Things
KPI	Key Performance Indicator
LoRA	Long Range
M2M	Machine to machine
ML	Machine Learning
mMTC	massive Machine-Type Communications
MNO	Mobile Network Operator
NB-IoT	Narrowband IoT
NF	Network Function
NG-IoT	Next-Generation IoT
NR	New Radio
NSA	Non-standalone
OPEX	Operational Expenditure
RIA	Research Innovation Action
SA	Standalone
SBA	Software-Based Architecture
SWOT	Strengths, Weaknesses, Opportunities and Threats
TRL	Technology Readiness Level
V2X	Vehicular to everything

Co-funded by the Horizon 2020
Framework Programme of the European Union

1. Introduction

This deliverable is the second report related to Task T2.3 of the iNGENIOUS project and represents a continuation of D2.3 [1]. The content is completely new, and both deliverables have been designed to complement each other. While D2.3 mainly captured the regulatory matters of the project, as well as a first analysis on the potential business models that could be derived from it per use case, D2.5 focuses on a more advanced business analysis, extracted from a series of questionnaires sent to key players in the IoT and related vertical industries.

The objective is to evaluate the main risks, obstacles and opportunities of our market-ready components and project developments. Note that there is no general business model for the architecture described in D2.2 as a whole, but specific business plans for those components with high TRL, which are listed in Section 4.

The following sections describe the main objectives of the project concerning these aspects, as well as the structure of the document.

1.1. Objectives

The creation of viable business models is essential for the deployment and evolution of the use cases demonstrated in iNGENIOUS. The use of next generation IoT technologies in the considered trials have the potential to create value for all stakeholders involved in the ecosystem. The project aims at digitalising and monitoring the whole supply chain ecosystem, starting by automating tasks in factories, continuing by tracking the transportation of assets and ending with automation of maritime port operatives. The main aim of iNGENIOUS was to bring to such players the necessary tools to further develop their business opportunities. Thanks to D2.5, we will understand if this need was covered during the course of the project.

The four main objectives of this deliverable are:

1. Describe the end-to-end iNGENIOUS ecosystem.

IoT technologies can be successfully adopted in industrial scenarios in various ways. However, in all cases, the fundamentals include, on the one hand, the ability of the provided IoT solutions to meet both operational and technical requirements, and on the other hand, the viability of business models to carry them out. In this sense, iNGENIOUS provides a study into the nature of our ecosystem and the underlying business drivers. The document describes in Section 2 the main findings resulting from this study.

2. Understand the needs and expectations of vertical stakeholders.

It is also key to study and understand the needs of the industry, in order to design, develop and provide the required products accordingly. In order to do so, this document explains in Section 3 the respondents' knowledge and experience in this field, their preferred solutions and IoT features for adoption, and their perspective on the maturity of the technology and its value to improve efficiency in some industrial processes. The objective is also to

Co-funded by the Horizon 2020 Framework Programme of the European Union

understand the main security and privacy challenges, and their key requirements (as discussed in objective 1).

3. Provide a business analysis of the iNGENIOUS portfolio.

The third objective is to analyse and study the different outcomes coming from the IoT solution providers questionnaire. The first task is to understand the iNGENIOUS product offering, that is, the solutions provided, our main innovation and differentiating attributes, as well as the level of maturity of such technologies. The second task is to focus on the marketing plan of each of the described solutions. We would like to see mainly who the potential customers and main competitors are, as well as the niche market that each product or prototype is covering.

4. Study the alignment between solution providers and the industry.

The last objective consists of understanding the level of alignment between both players, i.e., solution providers and stakeholders. This will be done in Section 4, where some key results will be compared against those obtained Section 3. Some examples are the perspective on the maturity level of IoT technologies, or the preferred/adopted solutions. More details on the different chapters of the document are provided next.

1.2. Structure

The document is structured in three main chapters, directly related to the four objectives mentioned in Section 1.1.

- **Section 2 (Ecosystem)** describes the iNGENIOUS end-to-end service chain (objective 1), including spectrum regulators, operators, infrastructures, and service providers, as well as application developers and integrators.
- **Section 3 (Stakeholders' vision: advanced business models for IoT)** shows the different answers provided by external vertical stakeholders and consortium members with a similar vision (objective 2). It also analyses their perspective and discusses the main outcomes of the questionnaires.
- **Section 4 (Solution providers: the iNGENIOUS approach)** explores the results obtained from the second questionnaire (objective 3) and compares them to the first one, extracting conclusions aligned with the fourth objective of the document (objective 4).

Finally, the main findings of this deliverable regarding these fields are provided in **Section 5 (Conclusion)**. Additionally, the complete questionnaires and their options sent to involved companies are provided in **Annex A**.

Co-funded by the Horizon 2020 Framework Programme of the European Union

2. Ecosystem

The IoT market is not limited to a few players. New actors, roles and relationships are constantly evolving and becoming part of the IoT ecosystem. In this section, we provide a brief study that analyses the nature of our ecosystem and its underlying business drivers. This will serve us as the context to understand the other two main sections of the document, where all these players come into play.

In particular, D2.5 will analyse how roles are distributed. Normally, some roles are closely associated to a particular actor. However, others may be associated to different actors, or even some actors can take different roles. In the iNGENIOUS ecosystem, we have identified **four main roles**, depicted in Figure 1.

- Spectrum regulators
- Infrastructure providers
- Technology solution providers
- Vertical stakeholders

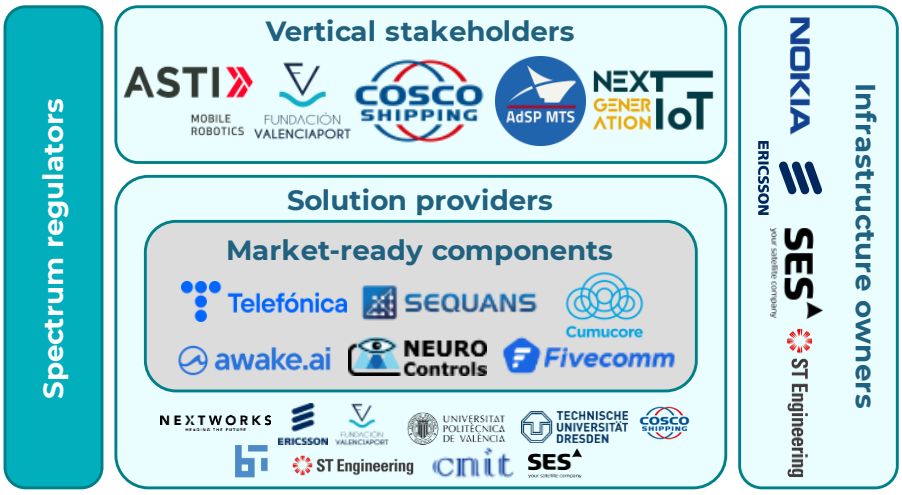

Figure 1. The iNGENIOUS ecosystem.

Although most of these roles are directly related to partners of the consortium, others are external players, whose involvement has been necessary for the execution of the project (e.g., spectrum regulators for trials, or other vertical stakeholders for the elaboration of this deliverable). Note that in later sections we focus on those technology solution providers with market-ready components (Section 3) and vertical stakeholders (Section 4), since they represent the core of this analysis.

2.1. Spectrum regulators

Spectrum is a limited natural resource and therefore its use needs to be controlled and legally assigned. Spectrum is usually managed and assigned by national regulators and administrations while considering the decision made at regional and/or international level [2].

Co-funded by the Horizon 2020 Framework Programme of the European Union

Spectrum licenses are key when performing trials, providing a particular wireless service to users, verticals, etc. Spectrum is used to support many applications and services, not only in mobile networks but also in satellite or broadcasting communications. For this reason, in order to avoid potential interferences and coordinate such large number of services, regulators come into play. They are in charge of the establishment of licenses and decide how spectrum is allocated in a particular country. The different types of spectrum licensing are provided in detail in D2.3 [1]. More detailed information can be also found at the ITU-R Report SM.2093-3 [3].

In the particular case of iNGENIOUS, coordination and collaboration with **external regulators** and satellite / mobile network operators (MNOs) has been necessary in the context of several use cases in order to obtain the required license and perform the trials accordingly. Examples are the industry use case (band 40 for private networks in Burgos) or the AGV use case (mm-wave spectrum in the Port of Valencia).

2.2. Infrastructure providers

These companies are generally the owners of a specific network infrastructure or part of it. The infrastructure provider is in charge of hosting not only the network elements such as the radio and core network, but also other components, e.g., lamp posts, antennas, power supply, etc.

iNGENIOUS has in the consortium **four infrastructure and network providers**, i.e., Nokia as one the main infrastructure owners in Europe and the main responsible of the infrastructure deployment in the Spanish facilities for the trials; Ericsson as the other main infrastructure provider in Europe; SES, who is using the project outcomes to optimise its new space segment and associated ground networks; and iDR, who has used the project as a gateway for indirect and direct access to IoT devices over satellite networks.

2.3. Technology solution providers

The integration of different IoT and related technologies into the main infrastructures across the vertical facilities within a single consortium has been one of the main focuses in iNGENIOUS. This has led us to the creation of new business models for the NG-IoT solutions for the universal supply chain.

Thanks to iNGENIOUS, several partners in the consortium have improved (or even developed from scratch) their products and services in new and existing markets. In total, there is large number of exploitation elements and components that have been developed in the context of the project, which will be reported in D7.3 [4]. In this deliverable, we focused on the **seven components** with a higher TRL and a clear market-oriented perspective. Such components are actually being commercialized or about to reach the market. The specific technology solution providers responsible for those components are NeuroControls, Fivecomm, Cumucore, Telefonica, Sequans and Awake AI. Note that other companies such as Nextworks, iDR, SES, FVP, UPV, CNIT, Ericsson, COSCO or BI have also reported some exploitable elements in D7.3, but their products will not be launched to market, so they are out of the scope of this deliverable. This differentiation can be also observed in Figure 1.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Note that, as stated before, some actors can take different roles. This is the case of SES, who can be considered an infrastructure provider, while also being a technology solution developer. Other examples are FVP (technology provider and stakeholder), Ericsson (infrastructure and solution provider), COSCO (technology provider and stakeholder), and iDR (infrastructure and solution provider).

2.4. Vertical stakeholders

The iNGENIOUS project embraces the vision of empowering smart manufacturing and smart mobility verticals through the development, integration and validation of the technology solutions presented in Section 4. Thanks to the project, vertical stakeholders have been able to implement progressively new IoT technologies in their systems, define the marketing actions and the necessary documentation to market such technologies in their services, and introduce them to potential customers in professional events and other contracts.

The project counts on **four vertical stakeholders**, i.e., ASTI-ABB, COSCO Spain, Autorità di Sistema Portuale del Mar Tirreno Settentrionale, and Fundación Valenciaport. The vertical sectors represented in iNGENIOUS are also supported by a strong external Advisory Board (AB). Note that these two pillars, together with other vertical companies from other NG-IoT projects, have participated in this particular deliverable (Section 3).

Co-funded by the Horizon 2020
Framework Programme of the European Union

3. Stakeholders' vision: advanced business models for IoT

This section provides an in-depth analysis of the results obtained from the questionnaire devoted to vertical stakeholders that currently use or plan to use IoT technologies. Using this analysis, we would like to understand their view on the industry and the enabling role of such technologies in their processes. The main conclusions to be extracted are related to the applicability of IoT products on their strategic and technology investments.

The main outcomes of this analysis are the following:

- Understanding of the IoT penetration and maturity in their industries.
- Main expectations from vertical stakeholders.
- IoT value compared to other previous wireless technologies.
- Social and commercial impact.
- Security and privacy aspects.

In order to obtain a clear representation of the verticals of interest, as a well as a wide picture of the entire NG-IoT network, the iNGENIOUS project contacted the following members[1] to answer the questionnaire:

A. iNGENIOUS consortium: **main use case actors**
    a. Fundación Valenciaport
    b. ASTI mobile robotics (now ABB)
    c. COSCO
B. **Advisory board** members: Port authority of Valencia.
C. External stakeholders from **other RIA NG-IoT projects**:
    a. Intell-IoT: Siemens
    b. VEDLIoT: Veoneer
    c. TERMINET: PPC, Megval
    d. IoT-NGIN: ABB, ASM Terni
    e. ASSIST-IoT: CIOP

A more illustrative picture describing all participants is shown in Figure 2. In total, 12 answers were received from a total of 11 companies.

The questionnaire (provided in Annex A), and therefore the analysis, has been divided into three main parts. The first section is directly related to the role of IoT in the industrial verticals, i.e., their knowledge about the technology and

[1] *Note:* other companies were also contacted but no response was received.

Co-funded by the Horizon 2020 Framework Programme of the European Union

its value, their preferences when deploying real solutions, and their maturity level. The second part focuses on other aspects, expected features and requirements. The third part consists of a SWOT analysis where all answers are compiled and harmonized in a single table.

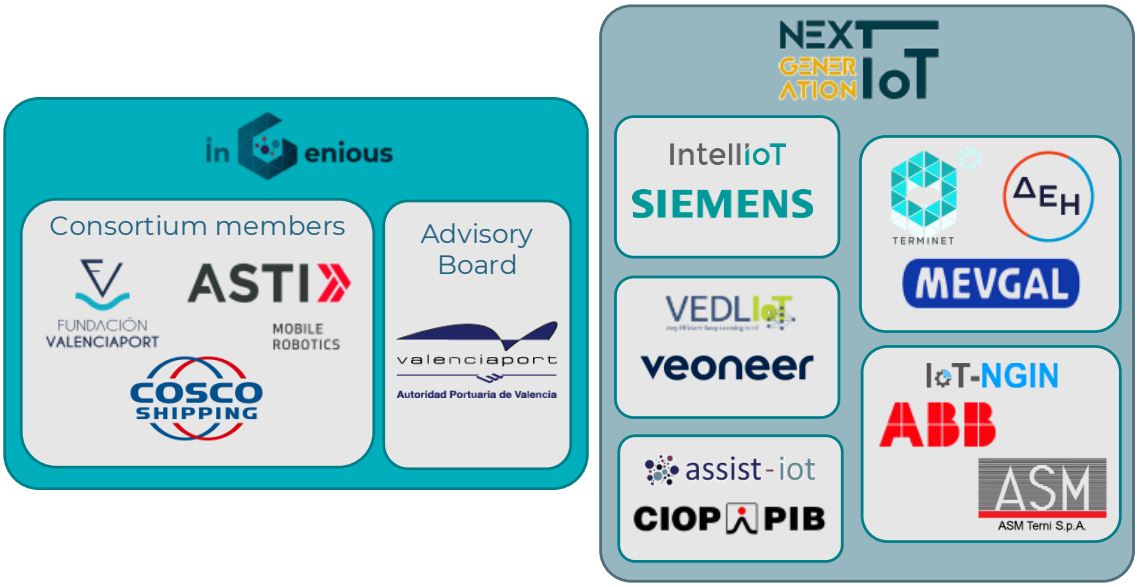

Figure 2. Vertical stakeholders that participated in this analysis.

3.1. IoT role in the industry

3.1.1. IOT KNOWLEDGE AND EXPERIENCE

The first step in knowing the vertical stakeholders' perspective consisted of understanding their knowledge about the field and the technology under study. For this reason, the following question was asked.

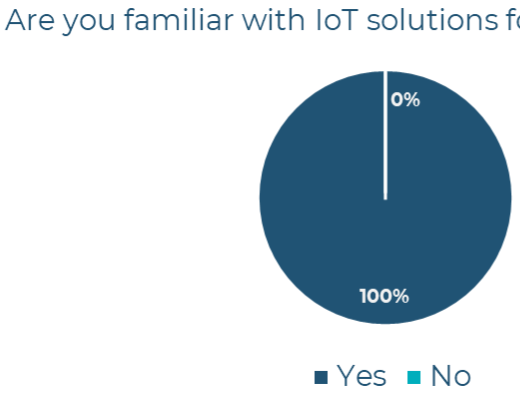

Figure 3. Vertical stakeholders' view: technical knowledge about IoT technologies.

As shown in Figure 3, **all vertical stakeholders** are familiar with IoT technologies. This is an important starting point for the analysis, as it could have changed our perspective when analysing the results. In the following figure, stakeholders were asked about the implementation and deployment of such technologies.

Co-funded by the Horizon 2020 Framework Programme of the European Union

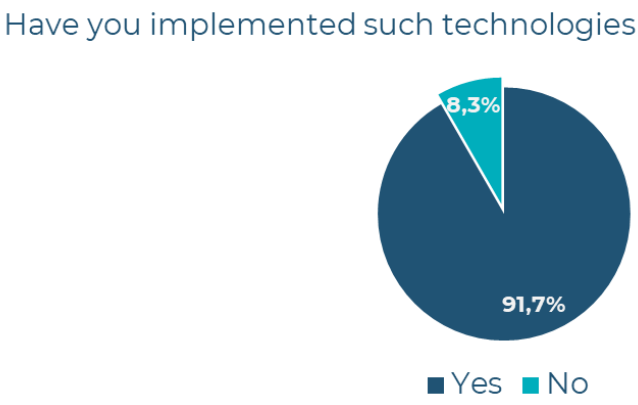

Figure 4. Vertical stakeholders' view: level of implementation of IoT solutions.

As it can be observed in Figure 4, the **91.7%** of stakeholders have already implemented at least one IoT solution in their premises. This means that there is a high-level of penetration already. In general, we can affirm that the level of knowledge and experience coming from stakeholders is high.

3.1.2. IOT VALUE TO IMPROVE EFFICIENCY IN INDUSTRIAL PROCESSES

The third question asked to interviewees was the following:

"Which value will IoT provide to improve efficiency in your industrial processes, if any?"

In general, all responses followed the same trend. IoT technologies will help industrial stakeholders to improve safety at work, industrial automation, and monitoring of industrial processes. It also will improve customers' satisfaction thanks to the use of track and trace, with easy remote access to reading status and alarms/events data from a plant. IoT devices are also useful for other industrial activities such as remote control of robotic systems, or Automated Guided Vehicles (AGV) monitoring and control.

In the particular case of ports, IoT may be also useful to exchange and monitor data in real time as container position and cargo status. It mainly increases the visibility in port processes which provides valuable information to evaluate the performance of these processes and, if necessary, apply actions to optimize them.

There is a particular answer that comes from ASM Terni, where as a distribution system operator, they think that the use of IoT devices increases the amount of data available, allowing operators to make decisions based on the real state of the network, as well as to detect faults quickly and gives the possibility to include analytical tools in the network management to increase performance (forecasting models, predictive network maintenance, etc.).

3.1.3. PREFERRED IOT SOLUTION FOR ADOPTION

There are several options for IoT connectivity, and it is clear that some particular alternatives have gained momentum and will garner the biggest share of the market in the following years. Depending on the industrial needs

Co-funded by the Horizon 2020 Framework Programme of the European Union

(energy efficiency, coverage, latency, etc.), there are many solutions that can serve as the ideal technology to cover such requirements. Examples are 4G and 5G-based technologies such as NB-IoT, CAT-M1, or NR, as well as LoRA, Sigfox, and others. In this context, stakeholders were asked about the type of IoT technology that they would prefer to adopt or are actually currently adopting.

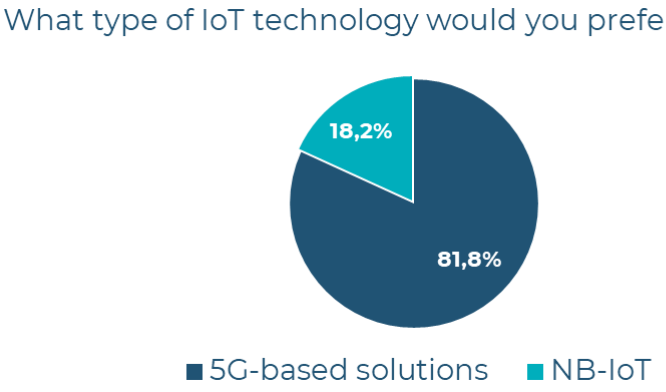

Figure 5. Vertical stakeholders' view: preferred IoT technology to adopt.

Interestingly, as shown in Figure 5, **81.8%** of them selected **5G-based solutions**, over a 18.2% that chose NB-IoT as the technology to use. Note that other alternatives, such as LoRA, Sigfox or Wi-Fi (some of them are offered within the iNGENIOUS portfolio as explained in Section 4.1.3) were not selected. As mentioned before, this most likely comes from the actual needs of the companies that answered the questionnaire.

3.1.4. MATURITY LEVEL OF IOT TECHNOLOGIES

Another important aspect to know when analysing a technology is its level of maturity and penetration in the current market. From the stakeholders' point of view, as shown in Figure 6, IoT technologies are far from their peak. They think that the current level of maturity is **average-high**, compared to other similar technologies.

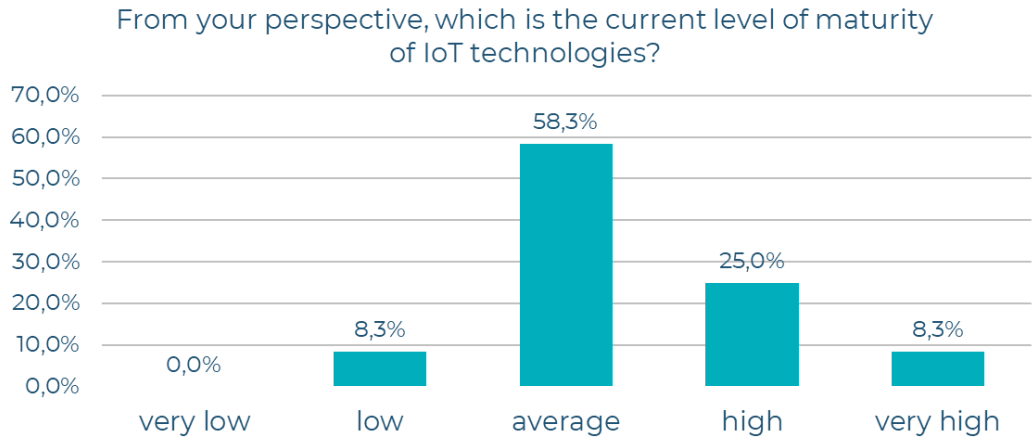

Figure 6. Vertical stakeholders' view: current level of maturity of IoT technologies.

On a score from 1 to 5, stakeholders have rated the level of IoT maturity as **3.3**, slightly above the average. Therefore, one can see that they still expect an

Co-funded by the Horizon 2020 Framework Programme of the European Union

evolution and grow of such technologies in the coming years, although some of them already think that the level of penetration is high. In fact, when asked about the time for general adoption, they answered the following.

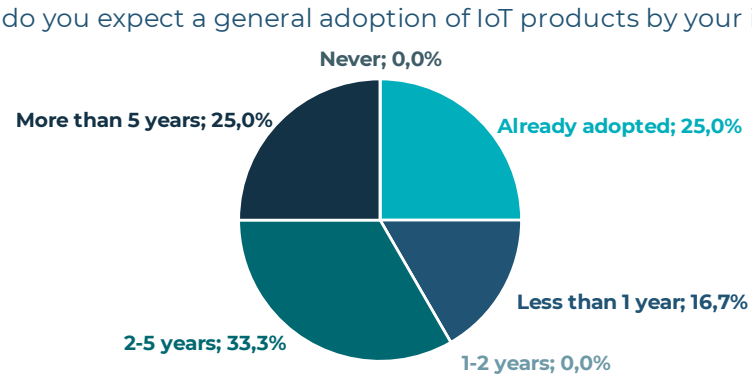

Figure 7. Vertical stakeholders' view: expected date for IoT adoption.

As depicted in Figure 7, **41.7%** of the stakeholders have already adopted some type of IoT product in their premises or will do so in less than one year. This is very well aligned with the results obtained in Figure 6. The other **58.3%** are thinking about adopting IoT solutions in a time frame of 2 or more years. In general, the interest level of stakeholders observed is high, especially considering that no answer was received in the '*never*' option.

3.2. Expected features and requirements

Once the position of vertical stakeholders on their interest about IoT and their preferred solutions was clear, they were asked about some other (more detailed) features and requirements that are expecting. The following analysis can be extracted.

3.2.1. SECURITY AND PRIVACY CHALLENGES

The first topic to cover is the security and privacy related challenges. On the one hand, it is well known that wireless networking is prone to security issues. The lack of a physical connection makes wireless technologies vulnerable to eavesdropping, hacking and other security issues. On the other hand, the protection of personal data is an issue that, especially in the recent years, has become central to the European legal landscape. The protection of personal data is fundamental to the protection of privacy.

Related to this topic, the following question was asked to the stakeholders.

What are the security and privacy challenges that IoT technologies need to overcome?

Some of them were highly concerned about data sharing, since there is a risk that data may be stolen. In terms of security, IoT technologies should be resilient against intrusions and potential hijacking attacks. Another concern was the authentication methods for encrypted communication. Security must also be very high for automotive safety applications.

Co-funded by the Horizon 2020 Framework Programme of the European Union

In terms of privacy, IoT technologies should be as much as off-the-shelf GDPR compliant as possible to avoid additional work on solving privacy constraints. Data ownership, device identity, user identity and tools' identity are some of the main concerns on this aspect. User acceptance (especially in work environment) is also a hot topic.

3.2.2. PREFERRED NETWORK AND IOT FEATURES

The following section is directly related to the 5G-based IoT technologies. The first question was about the use of private or public networks. Private networks provide mobile services for a dedicated and clearly defined set of users or 'things' that are usually part of a single organisation. They can provide the support needed to implement the mobile broadband requirements requested by the manufacturing sector to enable the Industrial Internet of Thing (IIoT) service implementation.

In contrast to a public network, which offers mobile network services to the public audience, a 5G private network provides 5G services to a clearly defined user organisation or group of organisations. On the other hand, the use of a public network significantly reduces both OPEX and CAPEX costs, while also providing wider coverage. In this context, stakeholders were asked about their preferences.

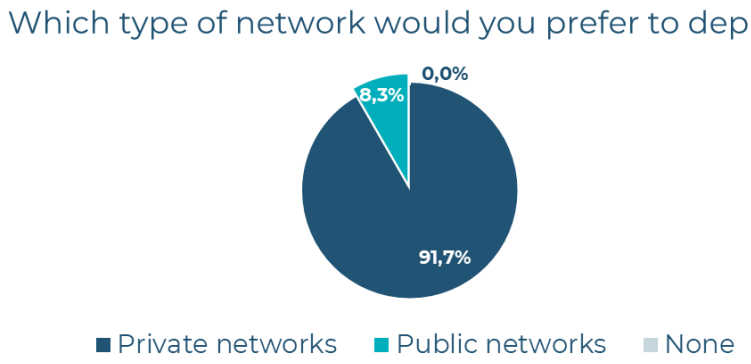

Figure 8. Vertical stakeholders' view: preferred type of network deployment.

As it can be observed in Figure 8, **91.7%** of the interviewees prefer a private network deployment over a public one. This is aligned with our expectations since vertical stakeholders are clearly the target for this type of network deployment. The only stakeholder that preferred public over private networks was related to the automotive vertical. Naturally, public networks offer wider ranges of coverage, which may facilitate the execution of V2X use cases.

Regarding the use of specific 5G-related features on their premises, interviewees answered the following.

Co-funded by the Horizon 2020 Framework Programme of the European Union

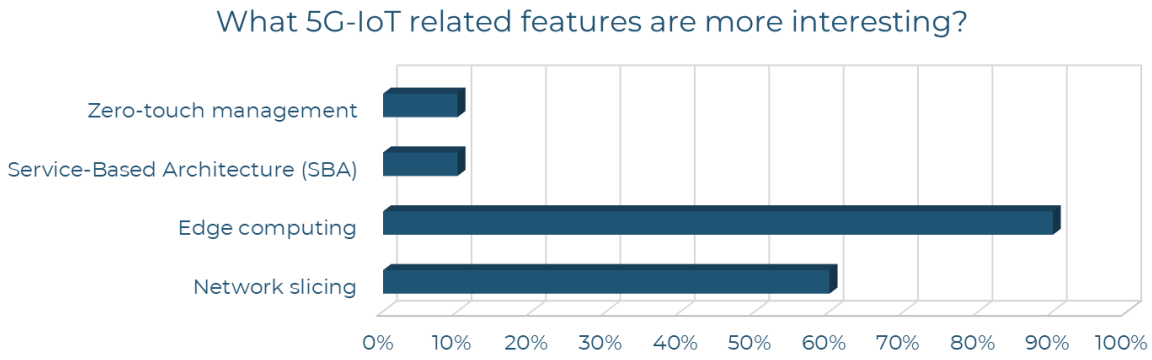

Figure 9. Vertical stakeholders' view: other related features that are of interest.

There is a clear interest in two main technologies, i.e., **edge computing** (90%) and **network slicing** (60%). Edge computing is a distributed technology that processes the client data at the outside edge of the network, as close to the transmitting/receiving source as possible. This naturally reduces drastically the end-to-end latency, which of course is of interest for vertical stakeholders, whose are applications are low-latency driven. The other most selected option is network slicing.

Network slicing allows to create logical networks with appropriate network and cloud resources, isolation, and optimised topology to provide customised services for vertical industries and use cases, while meeting their specific performance requirements. This is a great alternative for dedicated services, which makes the technology highly interesting for verticals.

The other two selected options are Service Based Architecture (SBA) and zero-touch management. SBA is a particular 5GC architecture that provides a modular framework, where common applications and interconnected Network Functions (NFs) can be deployed. It allows for cloud-native architectures and provides an agile, flexible, and scalable network technology achieving a software-defined 5GC. This particular option may be of interest to industrial verticals. On the other hand, zero-touch management is a fully autonomous network management solution that only needs human oversight [5]. In this sense, the network can understand its current state, interpret it, and provide recommendations about possible reconfigurations. This also may be of interest for some industrial cases such as ports or shopfloors.

3.2.3. KEY REQUIREMENTS

Once the vertical preferences on specific features are clear, we then analyse the most stringent requirements when deploying IoT services in their premises. Figure 10 shows the distribution of importance for five Key Performance Indicators (KPIs) that are of interest for such services, i.e., bandwidth (throughput), latency, connection density, energy efficiency and reliability.

Co-funded by the Horizon 2020 Framework Programme of the European Union

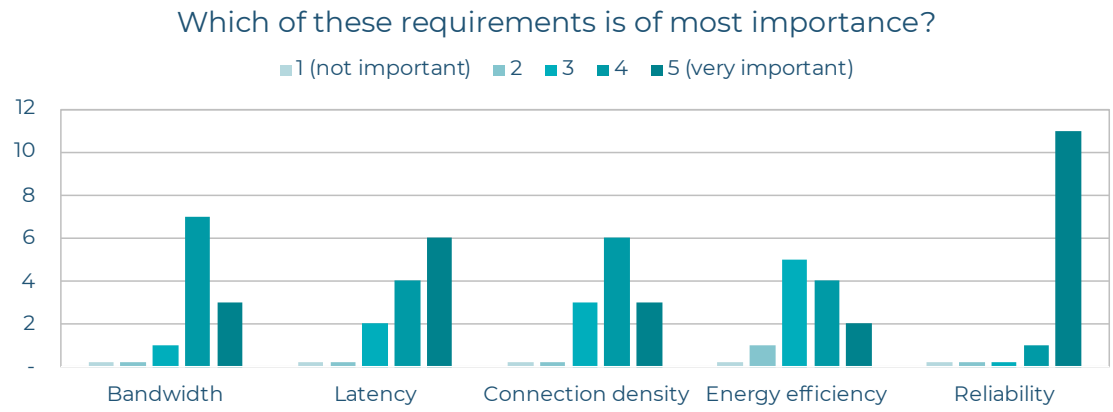

Figure 10. Most stringent requirements envisaged by vertical stakeholders.

From this figure, one can clearly see how **reliability** is the most important requirement when deploying an IoT system. This is well aligned with the 3GPP vision on mMTC (*massive Machine-Type Communications*), where such a requirement is the main focus. 11 out of 12 stakeholders think that it is of highest importance. Reliability has got a score of **4.91**.

The second selected requirement is latency, with a score of 4.33. This is also aligned with the selected options in Section 3.2.2, with a high predominance of edge computing and network slicing (technologies that actually enable low-latency services).

After reliability and latency, the next requirements are connection density and bandwidth with a score of 4.00. Connection density is also an important aspect when deploying many devices in an industrial environment. Bandwidth may be of importance as well, especially in video-related applications. The least valued KPI was energy efficiency, which obtained a score of 3.58. This low score is due to the nature of the interviewed verticals being ports or industrial partners, rather than utilities or related sectors.

3.2.4. OTHER ASPECTS

This subsection shows the stakeholders' vision about other aspects related to the use of wireless technologies. The first question about this topic was the following:

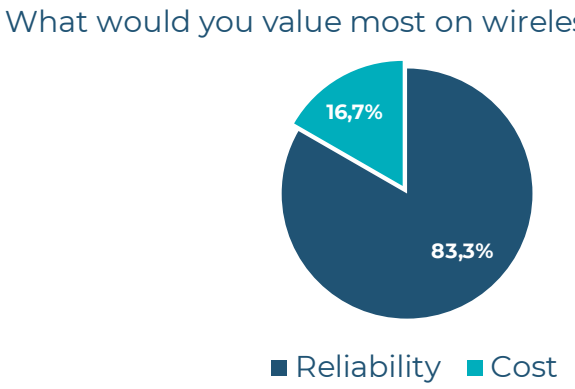

Figure 11. Vertical stakeholders' view: reliability vs. cost.

Co-funded by the Horizon 2020 Framework Programme of the European Union

When asked about the selection of reliable services over cost, verticals clearly selected a high reliability despite the fact that it may entail a higher cost. Stakeholders are eager to invest money in such technologies, as long as the system is reliable and robust. This vision is again aligned with the previous results obtained throughout the document.

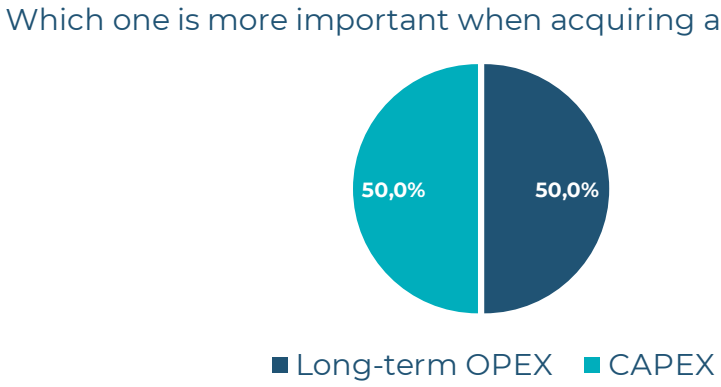

Figure 12. Vertical stakeholders' view: OPEX vs. CAPEX.

In terms of their preferences for acquiring a wireless solution, vertical stakeholders are clearly divided when investing. Half of them prefer to invest in long-term OPEX, that is, operational cost such as deploying end-to-end services, while the other half prefer to invest in CAPEX, putting the focus on infrastructure and equipment.

3.3. SWOT analysis

The last part of Section 3 provides a SWOT (Strengths, Weaknesses, Opportunities and Threats) analysis that compiles and assesses the use of new IoT solutions by verticals' businesses. It provides a comprehensive view on the main aspects related to the adoption of IoT technologies, from a vertical stakeholder point of view. In Table 1, all answers received in the questionnaire have been harmonized to better provide this view.

Strengths	Weaknesses
- Reliability. - Flexibility. - Scalability. - High coverage, with high widespread diffusion throughout the territory. - Real-time application. - Eased remote access, reutilization of previous works - Easy to use, cost-effective and innovation. - Minimisation of human effort.	- Security. - Low reliability if not implemented correctly. - Lack of or slow standardization processes. - Operating Cost. - Maturity. - Interoperability issues. - Sometimes unclear data ownership and data localization.

Co-funded by the Horizon 2020 Framework Programme of the European Union

- Existing standardized infrastructure. - Eased deployment, time reduction and number of devices - Access to data. - Autonomous operation. - Better monitoring of processes.	- The big number of different ontologies and messaging protocols usually requires additional resources in integration tasks. - Data will sometimes be sent outside system control. - Technical complexity. - Big investment needed.
Opportunities 	**Threats** 
- Many use cases for infrastructure management. - New services and business models. - Combination with big data and AI deployments. - Real time monitoring. - Predictive maintenance. - Collection of big amounts of data. - New work methodologies. - Real-time data exchange. - Increased visibility in all processes, which provides business insights to optimize the overall performance of the organization applying IoT. - Greater processing capacity and data gathering from multiple sources. - Virtualisation. - Data governance. - Multi-stakeholder involvement and collaboration.	- Eavesdropping, hacking and other security issues. - Data integration. - Obsolescence of sensors. - Low reliability may happen. - Loss of data - There is still room for improvement regarding security. IoT devices and integrations are not exempt of ransomware, spyware, or other forms of malware. - Malicious actors - Data leakage

Table 1. SWOT analysis of IoT technologies from a stakeholder perspective.

Co-funded by the Horizon 2020 Framework Programme of the European Union

4. Solution providers: the iNGENIOUS approach

This section provides an in-depth analysis of the results obtained from the questionnaire (Annex A) devoted to the iNGENIOUS solution providers, which have developed or are developing them in the context of the project. The idea is to study their role and vision and compare it to the one provided by stakeholders in Section 3.

The main outcomes of this questionnaire are the following:

- Social and commercial impact of our products.
- Level of scalability and penetration into the market.
- 5G-IoT value compared to other wireless technologies.

The products selected for this questionnaire are market-ready components with a clear exploitation plan, that is, those that have gone or will go to the market soon as a product. We have considered the following components:

1. Micro-edge ML-enabled sensors, GW, and AI data loggers (NCG)
2. 5G modem (Fivecomm)
3. Industrial 5G core (Cumucore)
4. Cross-DLT solution (Telefonica)
5. 4G and 5G chipsets and modules for cellular IoT (Sequans)
6. Cloud-based analytics services predicting port traffic rates and truck turnaround times (AWA)
7. 5G based immersive cockpit (Fivecomm)

As done in Section 3, this analysis has been divided into three main parts. The first section covers aspects related to the product offering, that is, the main innovation, particular IoT technology used and maturity level. The second part is about the market identification of such solutions, covering not only the main competitors, but also the potential customers and niche market. Finally, in the third part we provided a SWOT analysis per component that will help to understand the business model of each of them.

4.1. Product offering

4.1.1. MAIN INNOVATION

The first and most important element to analyse from our products is their main innovation, i.e., the novelty with respect to the competence. In order to get this information, we asked the following to the solution providers:

Why do you think this product/service is needed?

Co-funded by the Horizon 2020 Framework Programme of the European Union

Table 2 compiles the different innovations of the components analysed in this deliverable.

IoT solution	Partner	Main innovation
Micro-edge ML-enabled sensors, gateways, and AI Data Loggers	NCG	Edge sensors drive digitalization. AI data loggers accelerate data science projects
5G modem	5CMM	It is needed to provide 5G connectivity to different industry verticals given its adaptability which can satisfy the needs of multiples industries with specific needs.
Industrial 5G Core	CMC	Vendors have designed and developed 5G core for consumer market and there is no 5G Core designed specifically for non-public industrial networks.
Cross-DLT solution	TIOTBD	It integrates different DLTs as trust mechanisms for information exchange in the supply chain. The main aim of this solution is to provide an interoperable layer in order to abstract the complexity of the underlying DLT solutions, guaranteeing at the same time data privacy and security by means of encoding and anonymization techniques.
4G and 5G chipsets and modules for cellular IoT	SEQ	Needed for efficient, robust, and secure communication in every kind of IoT applications
Cloud-based analytics services predicting port traffic rates and truck turnaround times	AWA	It is useful for port authorities, city traffic planning, hinterland carriers, and cargo owners to be able to predict e.g., future congestion periods at the port.
5G based immersive cockpit	5CMM	The immersive cockpit of Fivecomm is needed to support new 5G use cases that require advance network applications, mainly related to advanced remote and autonomous driving services. It can be a key solution in particular vertical scenarios such as ports or industrial shop floors, inspection of critical infrastructures, dangerous places for human beings, or simply for remote driving in case of human unavailability or ailment.

Table 2. Solution providers' view: main innovation of components.

4.1.2. DIFFERENTIATING ATTRIBUTES

A second question related to the same topic was about the differentiating attributes that make our products unique. In particular, our IoT solution providers answered the following.

Co-funded by the Horizon 2020 Framework Programme of the European Union

How is the product/service different than what is already out there?

Table 3 compiles the differentiating attributes of the components.

IoT solution	Partner	Differentiating attributes
Micro-edge ML-enabled sensors, gateways, and AI Data Loggers	NCG	Self-Powered Micro-Edge is unique. It eliminates wired installation costs or alternative battery maintenance. This is valuable for both infrastructure and mobile based applications.
5G modem	5CMM	The Fivecomm solution is highly customizable. It comes with an open-source operating system that allows the integration of additional functionalities. In addition, the case and other characteristics such as the number of antennas can be adapted easily. It supports the integration of external sensors thanks to the general-purpose board integrated in the solution. The modem supports NSA and SA networks and a very high number of frequency bands and band combinations. It has been smoothly integrated in public and private networks all around Europe.
Industrial 5G Core	CMC	The 5G core is unique since includes features required for industrial networks such as 5GLAN, Time Sensitive Network and network slicing all combined with easy-to-use graphical interface to be managed similarly as Wi-Fi network but with the security, coverage, and reliability of mobile infrastructure.
Cross-DLT solution	TIOTBD	Many of the existing solutions do not have the capability of storing information along different DLTs regardless of the technology they use. The solution allows to increase trust and extend the reach of the project. The combination of multiple DLTs makes the solution attractive to a wider group of users as some will prefer some DLTs over others. It also provides a way to ensure and verify the integrity of information coming from different systems.
4G and 5G chipsets and modules for cellular IoT	SEQ	Optimised (power, cost, performance) for IoT applications of every type. Our expertise and years of experience in cellular IoT makes us uniquely able to help our customers through the various business and technical deployment challenges of cellular.
Cloud-based analytics services predicting port traffic rates and truck turnaround times	AWA	Port organisations and information systems currently operate in their own silos, and use of predictive models in operational planning is not yet common. This service produces new information by i) integrating data from multiple actors in the port supply chain in a holistic manner and ii) implementing machine learning

Co-funded by the Horizon 2020 Framework Programme of the European Union

		and predictive analytics based on multimodal data.
5G based immersive cockpit	5CMM	The software platform that forms the immersive cockpit is highly customizable and flexible. It can be adapted to the specific type of service that needs to be provided, and to different customers.

Table 3. Solution providers' view: differentiating attributes of components.

4.1.3. ADOPTED IOT SOLUTION

It is indeed important that our solutions and products are innovative and different from the competition. It is also true that the level of innovation and the specific competing companies may change depending on the particular technology the solution is based on. In order to study what iNGENIOUS is offering and understand the level of alignment with stakeholders' perspective, the following question was included in the questionnaire.

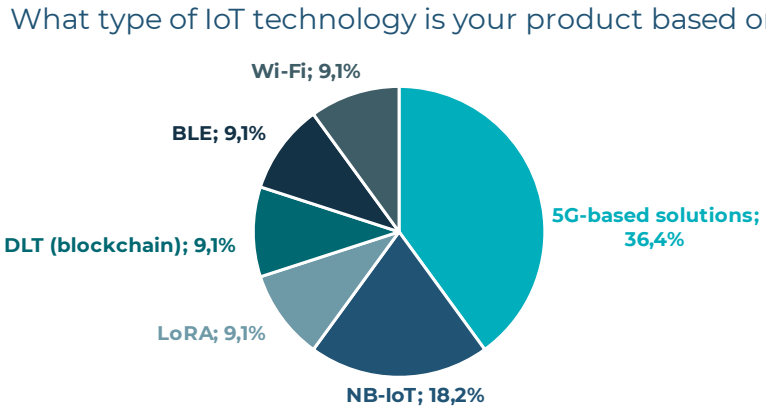

Figure 13. Solution providers' view: IoT technology in which products are based.

Observing Figure 13, and comparing with Figure 5 (included in Section 3.1.3), there is a wide offering with respect to types of technologies in our consortium. While vertical stakeholders are mainly interested in **5G-based** and **NB-IoT** solutions, these two alternatives represent the **54.6%** of our portfolio.

Partners in iNGENIOUS have also developed in the context of the project solutions based on LoRA, BLE (Bluetooth Low-Energy) and Wi-Fi, although only with a small partition of 9.1%. DLT (Distributed Ledger Technology) and blockchain are also part of the portfolio with another 9.1%.

4.1.4. MATURITY LEVEL OF IOT TECHNOLOGIES

Following the same idea than the previous section, our IoT solution providers were asked about the maturity level of their proposed technologies. Similarly, the idea is to compare their outcomes with the stakeholders' answers shown in Section 3 and understand the level of alignment between the two groups. First, Figure 14 shows the level of development of our products and prototypes.

Co-funded by the Horizon 2020 Framework Programme of the European Union

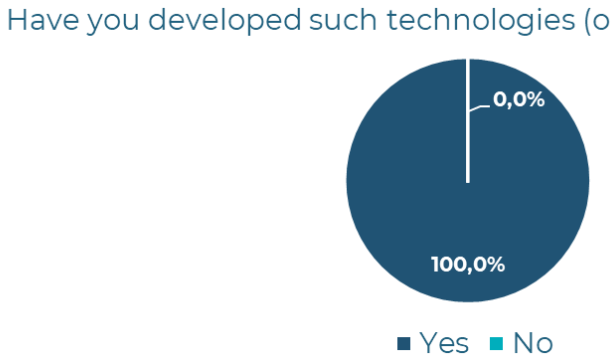

Figure 14. Solution providers' view: development status of their solutions.

As it can be observed, **100%** of our IoT solutions have been already developed in the context of iNGENIOUS. This is completely aligned with Section 3.1.1, since Figure 4 shows that **91.7%** of stakeholders have already implemented at least one IoT solution in their premises. This means that there is a high-level of penetration already, and therefore fully operational products are required.

Alternatively, in Section 3.1.4, vertical stakeholders were asked about their perspective on the maturity level of IoT technologies, obtaining a score of 3.3 out of 5. The same question was done to the solution developers. The results are shown in Figure 15.

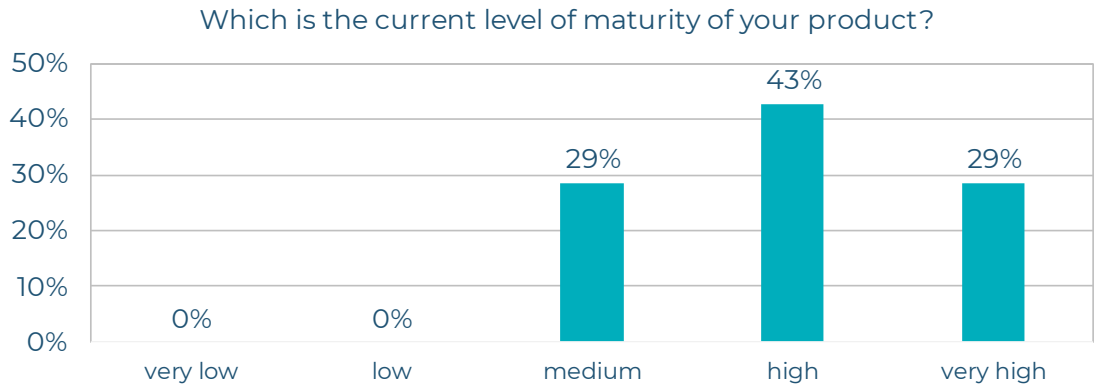

Figure 15. Solution providers' view: current level of maturity of IoT technologies.

The figure shows how, from a developer perspective, the maturity level of a technology usually becomes higher, since there is a better knowledge on the status of its development. In particular, the iNGENIOUS solution providers think that IoT is at maturity level of **4.0**, clearly higher than the other result (3.3).

A similar behaviour can be observed in Figure 16.

Co-funded by the Horizon 2020 Framework Programme of the European Union

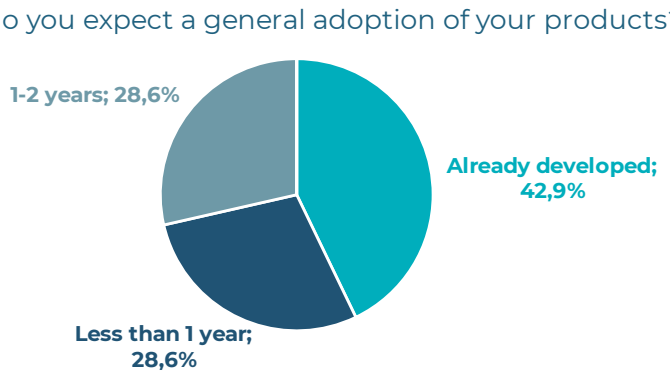

Figure 16. Solution providers' view: actual date of IoT products' launch to market.

The previous graph shows that **71.5%** of IoT solution providers are already delivering their products in the market or are expecting them to be adopted in less than one year. This is clearly higher than the 41.7% provided by stakeholders, again aligned with our expectations. Usually, developers expect their products to be adopted faster than the market is expecting. Interestingly, the rest of IoT providers expect their products to be adopted in less than 2 years. This is well aligned with the answers in Figure 14 and Figure 15.

In any case, one can affirm that the level of alignment between vertical stakeholders and our IoT products is relatively high, with a more optimistic perspective on our side.

4.2. Market identification

The following subsection describes the market identification of the iNGENIOUS solutions. Herein, we analyse the market to face, as well as our potential customers and competitors.

4.2.1. IOT MOMENTUM

The first point of this part of the analysis is related to the specific momentum of the IoT industry in the market. IoT solution providers responded to the following question.

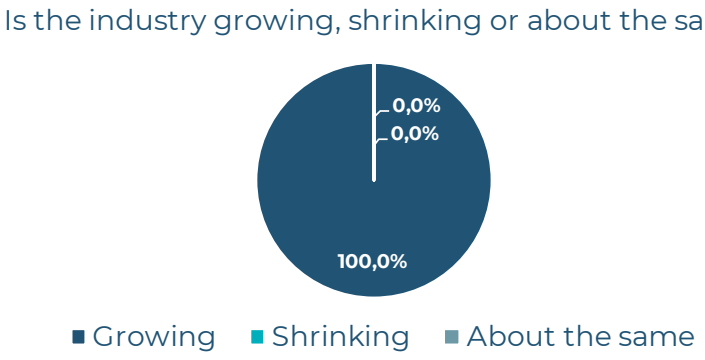

Figure 17. Solution providers' view on the IoT industry momentum.

Co-funded by the Horizon 2020 Framework Programme of the European Union

As shown in Figure 17, **100%** of our solution providers think that the IoT industry is currently growing. None of them think that the IoT industry is shrinking or will keep the same size in the next years. Naturally, companies invest in research and development of specific products when the potential industry under study is in full swing. Therefore, this answer is aligned with our expectations.

4.2.2. POTENTIAL CUSTOMERS

The following table depicts the potential customers of each of the IoT products offered by a single partner in INGENIOUS.

IoT solution	Partner	Potential customers
Micro-edge ML-enabled sensors, gateways, and AI Data Loggers	NCG	Rail, Industrial, Infrastructure, Product Validation Testing, General Data Science
5G modem	5CMM	Vertical industries such as robot manufacturers (mobile or fixed), agriculture, smart city managers (for smart mobility for example), etc.
Industrial 5G Core	CMC	Smart factories supporting industry 4.0, harbours, construction and other companies interested in having own private mobile infrastructure
Cross-DLT solution	TIOTBD	Any type of company, projects that need data immutability, trust, and security
4G and 5G chipsets and modules for cellular IoT	SEQ	Massive IoT product makers, broadband IoT product makers
Cloud-based analytics services predicting port traffic rates and truck turnaround times.	AWA	Port authorities, logistics operators, cargo owners, city traffic management operators, other system providers for the aforementioned.
5G based immersive cockpit	5CMM	Mobile network operators, vertical stakeholders such as ports or smart factories, inspection companies, robot manufacturers, mainly.

Table 4. Solution providers' view: potential customers of their products.

4.2.3. MAIN COMPETITORS

Potential competitors are mainly other companies that can offer a similar solution or service to the same type of customers. Knowing who the competitors are as well as their offering can help our consortium to understand how to develop our products and make them stand out. A competitor could be a new business offering, a substitute or similar product that makes your own redundant [6]. When asked about their competitors, project partners answered the following in Table 5.

Co-funded by the Horizon 2020 Framework Programme of the European Union

IoT solution	Partner	Competitors
Micro-edge ML-enabled sensors, gateways, and AI Data Loggers	NCG	Acoustic edge companies
5G modem	5CMM	Big players such as Huawei, Siemens are partially competitors, but do not usually focus on our niches. Other medium size players such as Teltonika are more focused on our target sectors.
Industrial 5G Core	CMC	New entrants
4G and 5G chipsets and modules for cellular IoT	SEQ	Qualcomm, Nordic, Altair
Cloud-based analytics services predicting port traffic rates and truck turnaround times.	AWA	Direct competitors include other digital solutions providers for maritime logistics, such as PortXchange, and maritime analytics companies such as Sinay. Multimodal transportation visibility service providers such as e.g., Shippeo may become customers or competitors.
5G based immersive cockpit	5CMM	Other cockpits have been developed in the context of H2020 projects such as 5G-MOBIX or 5G-CARMEN. Companies that have been working also in a similar product are Ericsson, Nokia, or DriveU, among others.

Table 5. Solution providers' view: main competitors of our products.

4.2.4. NICHE MARKET

It is also important to understand the market opportunities that each of the partners have foreseen when using IoT as a main technology. The niche market to address is of outmost importance. Table 6 shows the niche market of each individual product.

IoT solution	Partner	Niche market
Micro-edge ML-enabled sensors, gateways, and AI Data Loggers	NCG	Application-specific development
5G modem	5CMM	Our product is a 5G product, but we foresee its use for IoT services with high bandwidth and low latency requirements as the key opportunity. One case is connection of mobile robots.
Industrial 5G Core	CMC	Globally.

Co-funded by the Horizon 2020 Framework Programme of the European Union

4G and 5G chipsets and modules for cellular IoT	SEQ	Industry verticals (e.g., transportation, shipping, factories), and satellite-based comms.
Cloud-based analytics services predicting port traffic rates and truck turnaround times.	AWA	From a technical perspective, we anticipate availability of more varied, widely available, and frequently updated operational data along the various stages of cargo moving in the multimodal supply chain. This will enable providing our solutions in more locations, and developing more accurate models (i.e., better service quality) as the underlying data will improve in quality and coverage. However, there are still challenges in increasing the willingness of organisations to share mutually beneficial data across organisations for this kind of applications.
5G based immersive cockpit	5CMM	5G-IoT based connectivity enables the use of this product with very low latency and high throughput. We have tested the product with and without the use of such technology and the results show a clear improvement in the overall QoS. The use of haptic gloves and VR as key elements is also a great opportunity to enable new services.

Table 6. Solution providers' view: niche market of individual products.

4.3. SWOT analysis

As done in Section 3, this section provides a SWOT analysis to better define the main strong as well as weak points of our portfolio. The first SWOT analysis presented in Table 1 focused in the IoT technology as a whole, from a vertical perspective. Here, different tables are provided (Table 7 to Table 12), with a single table per individual component[2].

Micro-edge ML-enabled sensors, gateways, and AI Data Loggers	
Strengths	**Weaknesses**
Low Power moving to Self-Powered	Speed to Market
Opportunities	**Threats**
Customized Solutions	Pre-Financing Cash-Flow requirements

Table 7. Solution providers' view: brief SWOT analysis of micro-edge ML-enabled sensors provided by NCG.

[2] No SWOT analysis for the cross-DLT solution was provided.

Co-funded by the Horizon 2020 Framework Programme of the European Union

5G modem	
Strengths	**Weaknesses**
Compared to wired technologies, we offer mobility. Compared to wireless, Wi-Fi is not valid right now for the service requirements of the applications in which we are focused such as remote driving of mobile robots.	5G cost is now high and this is a weakness compared to other wireless technologies.
Opportunities	**Threats**
There is a high interest of the administrations and customers for advanced communication services not supported by previous technologies, and on 5G in particular. There are a lot of niche markets where the product offered by Fivecomm could be adopted.	The main threat is the competence from big and medium players well established in the market.

Table 8. Solution providers' view: SWOT analysis of the 5G modem provided by Fivecomm.

Industrial 5G core	
Strengths	**Weaknesses**
Secure and high availability of wireless communications. Larger coverage and support for seamless mobility.	Cost and complexity higher than other wireless technologies like Wi-Fi.
Opportunities	**Threats**
Private networks deployment for industrial usage, manufacturing, constructions, logistics, harbours, etc is new segment where major vendors are nor addressing because require specific tailoring of 5G technology, but it brings new segments and business opportunities compared to stagnant consumer market.	Fragmented availability of licensed frequencies allocated by the governments to non-public networks is fragmented and so far, only public mobile operators have the monopoly of licensed frequencies

Table 9. Solution providers' view: SWOT analysis of the industrial 5GC provided by Cumucore.

4G and 5G chipsets and modules for cellular IoT	
Strengths	**Weaknesses**
Reliable performance, secure, no requirement of new connectivity infrastructure, long-term support, future-proof, continuous evolution.	Cost for licensed spectrum resources, less flexible / simple deployment to extend existing network coverage.
Opportunities	**Threats**
Originally designed for broadband service, but now evolved (and keep evolving) to address any kind of IoT application.	To remain more costly or less flexible for deployment if specification does not evolve for optimising towards these directions.

Table 10. Solution providers' view: SWOT analysis of the 4G/5G chipsets from Sequans.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Cloud-based analytics services predicting port traffic rates and truck turnaround times.	
Strengths	**Weaknesses**
Widespread access to ubiquitous mobile sensors provides possibilities for new analytics services.	Many organisations in the maritime supply chain are slow to develop their digital systems, it may be difficult or slow to roll out new IoT services.
Opportunities	**Threats**
Responsible sharing of information derived from IoT sensor data can benefit many actors in the multimodal supply chain.	Sharing IoT data is seen as a threat or its added value is not identified, and the potential benefits are not fully realized.

Table 11. Solution providers' view: SWOT analysis of the cloud-based analytics services.

5G based immersive cockpit	
Strengths	**Weaknesses**
A 5G based immersive cockpit provides lower latency, increased reliability, and higher throughput that other wireless technologies such as LTE. Obviously, wired technologies cannot be used, since the vehicle needs to move around. Use of haptic gloves for remote control.	5G-IoT based technologies are still far from being optimized and therefore reliable.
Opportunities	**Threats**
New services and use cases can be created thanks to the use of this product. The haptic gloves are intuitive and reliable.	Strong competence, onboarding of peripherals in other advanced cockpits may not take a long time.

Table 12. Solution providers' view: SWOT analysis of the 5G based immersive cockpit.

Co-funded by the Horizon 2020 Framework Programme of the European Union

5. Conclusion

The present document, **D2.5**, has provided a deep business analysis of the IoT solutions developed within the context of the project iNGENIOUS. In order to do so, we first discussed the **iNGENIOUS ecosystem**, that is, the different actors involved in the project and their role in the end-to-end IoT chain. The identified key players are spectrum regulators, infrastructure owners, technology solution providers, and vertical stakeholders. This first analysis has been performed with the aim of understanding the context of the project and our main role in the IoT industry.

Once the ecosystem has been clearly defined, the document has focused on the **business analysis** itself. The analysis has been done from two different perspectives, i.e., from a vertical stakeholder point of view and from the iNGENIOUS project as IoT technology solution provider (i.e., the two main players in the ecosystem). Both visions have been obtained through two different questionnaires containing a wide variety of topics related to IoT and its ecosystem.

The questionnaire addressed to vertical stakeholders was sent and answered by members of the iNGENIOUS consortium, Advisory Board members, and external industrial companies from **all NG-IoT projects**, that is, Intell-IoT, VEDLIoT, TERMINET, IoT-NGIN, and ASSIST-IoT. Regarding the second questionnaire, it has been addressed to and answered by all partners with an exploitation element that has gone or will eventually go to the market as a product. The main objective of this document has been the complete understanding of the industrial needs, in order to design, develop and provide the required products accordingly.

5.1. Main outcomes from stakeholders

The first questionnaire was addressed to vertical stakeholders. Its main outcomes will be used as an input to improve our portfolio and provide products to satisfy the industry needs accordingly. From the questionnaire, we have seen that 100% of vertical stakeholders are **familiar with IoT** technologies. Actually, 91.7% of them have already implemented at least one IoT solution in their premises. This means that there is a high-level of penetration already among the interviewees.

When discussing the **IoT added value** to improve industrial processes, all answers followed the same trend. IoT technologies will help industrial stakeholders to improve safety at work, industrial automation, customers' satisfaction, or easy remote access, among others. IoT may be also useful to exchange and monitor data in real time.

The document has additionally covered the preferred solutions and IoT features for adoption. In this context, 81.8% of verticals selected **5G-based solutions**, over a 18.2% that chose NB-IoT as the technology to use. Other alternatives, such as LoRA, Sigfox or Wi-Fi were not selected.

We also wanted to know their perspective on the maturity of the technology and its value to improve efficiency in some industrial processes. On a score from 1 to 5, stakeholders have rated the level of **IoT maturity** as **3.3**, slightly

Co-funded by the Horizon 2020 Framework Programme of the European Union

above the average. Therefore, one can see that they still expect an evolution and grow of such technologies in the coming years, although some of them already think that the level of penetration is high. In fact, when asked about the time for general adoption, 41.7% of the stakeholders explained that they have already adopted at least one type of IoT product in their premises or will do so in less than one year.

When asked about **security**, some verticals were highly concerned about data sharing, resiliency against intrusions and potential hijacking attacks, or authentication methods for encrypted communication. In terms of **privacy**, data ownership, device identity, user identity and tools' identity are some of the main concerns. User acceptance (especially in work environments) is also a hot topic.

Talking about specific network deployments and alternatives, 91.7% of the interviewees preferred a **private network** deployment over a public one. This is completely aligned with our expectations since vertical stakeholders are clearly the target for this type of networks. In fact, they have shown a clear interest in edge computing and network slicing as well, which guarantee a specific QoS for a particular service.

Finally, they were asked about the most stringent requirements when deploying IoT services in their premises. **Reliability** has been clearly the most important requirement with a score of 4.91. The second selected requirement is latency, with a score of 4.33. The next requirements have been connection density and bandwidth with a score of 4.00. The least valued KPI was energy efficiency, which obtained a score of 3.58.

5.2. Main outcomes from IoT providers

As mentioned during the document, the second questionnaire was addressed to the IoT market-ready solution providers of our project. This has been done to understand the level of alignment between them and stakeholders' point of view. The first part of this analysis has provided a detailed description of the **iNGENIOUS product offering**, i.e., the solutions provided and their **innovation**, explaining how the products and services offered are different than what is already out in the market.

Concerning the level of adoption, **100%** of our IoT solutions have been already developed in the context of iNGENIOUS. This is completely aligned with the stakeholders' view, since **91.7%** have already implemented at least one IoT solution in their premises. This means that there is a high-level of penetration already, and therefore fully operational products are required.

As done with stakeholders, the analysis has covered the solutions and IoT features adopted in this case. Compared to the verticals' needs, there is a wide offering with respect to types of technologies in our consortium. While vertical stakeholders are mainly interested in **5G-based** and **NB-IoT** solutions, these two alternatives only represent the 54.6% of our portfolio. The iNGENIOUS offering is also based on LoRA, BLE, Wi-Fi, and blockchain.

About the maturity level of the proposed technologies, it has been observed how, from a developer perspective, the maturity level of a technology usually

Co-funded by the Horizon 2020 Framework Programme of the European Union

becomes higher, since there is a better knowledge on the status of its development. Interviewees in this case selected an **IoT maturity** level of **4.0**, clearly above the other result (3.3). Furthermore, 71.5% of our solution providers are already delivering their products in the market or are expecting them to be adopted in less than one year. It is indeed a higher number, compared to the 41.7% provided by stakeholders.

The second part of this analysis has covered the **market identification** of the different products analysed. It has covered mainly three aspects, i.e., the main competitors, potential customers, and niche market to cover. Specific detailed tables for each product have been provided throughout the document.

In general terms, one can affirm that the answers received in both questionnaires are aligned with the iNGENIOUS expectations. Both views are completely aligned, with small differences, and therefore it is safe to affirm that **our consortium is ready** to provide the products and services expected in the industry.

Co-funded by the Horizon 2020
Framework Programme of the European Union

References

[1] Manuel Fuentes, Miguel Cantero, "D2.3: Regulatory Framework and Business Models," iNGENIOUS, 2021.

[2] Digital Regulation Platform, "Spectrum management: Key applications and regulatory considerations driving the future use of spectrum," August 2020.

[3] Internation Telecommunications Union, "Report ITU-R SM.2093-4: Guidance on the Regulatory Framework for National Spectrum Management," 2021.

[4] Erin Seder, "D7.3: Final dissemination, standardisation and exploitation," iNGENIOUS, 2023.

[5] E. C. e. al., "Zero Touch Management: A Survey of Network Automation Solutions for 5G and 6G Networks," *IEEE Communications Surveys & Tutorials,* vol. 24, no. 4, pp. 2535-2578, 2022.

[6] Business Link UK (Adapted for Québec by Info entrepreneurs), "Understand your competitors," 2009.

Co-funded by the Horizon 2020 Framework Programme of the European Union

Annex A: Questionnaires

The iNGENIOUS vision: Advanced business models for IoT technologies (Section 3)

IoT role in the industry

1. Are you familiar with IoT solutions for your industry?
   - O *Yes*
   - O *No*
2. Have you implemented such technologies (or prototypes) already?
   - O *Yes*
   - O *No*
3. Which value will IoT provide to improve efficiency in your industrial processes, if any?

   Short answer
4. From your perspective, which is the current level of maturity of IoT technologies?

	1	*2*	*3*	*4*	*5*	
Very low	O	O	O	O	O	*Very high*

5. When do you expect a general adoption of IoT products by your industry?
   - O *Already adopted*
   - O *Less than 1 year*
   - O *1-2 years*
   - O *2-5 years*
   - O *More than 5 years*
   - O *Never*
6. What type of IoT technology would you prefer to adopt?
   - O *5G-based solutions*
   - O *NB-IoT*
   - O *LoRA*
   - O *Sigfox*
   - O *Others*

Co-funded by the Horizon 2020 Framework Programme of the European Union

Expected features and requirements

7. What are the security and privacy challenges that IoT technologies need to overcome?

   Answer

8. Which type of network would you prefer to deploy?

   - ○ *Private networks*
   - ○ *Public networks*
   - ○ *None*

9. Which of these requirements is of most importance? (1: not important, 5: very important)

	1	*2*	*3*	*4*	*5*
Bandwidth	○	○	○	○	○
Latency	○	○	○	○	○
Connection density	○	○	○	○	○
Energy efficiency	○	○	○	○	○
Reliability	○	○	○	○	○

10. What 5G-IoT related features are more interesting?

    - ☐ *Network slicing*
    - ☐ *Edge computing*
    - ☐ *Service-Based Architecture (SBA)*
    - ☐ *Others*

11. What would you value most on wireless technologies?

    - ○ *Reliability*
    - ○ *Cost*

12. Which one is more important when acquiring a wireless solution?

    - ○ *CAPEX*
    - ○ *Long-term OPEX*

SWOT Analysis

13. Strengths of IoT compared to other wireless/wired technologies:

    Short answer

14. Weaknesses:

    Short answer

15. Opportunities:

    Short answer

Co-funded by the Horizon 2020 Framework Programme of the European Union

16. Threats:

    Short answer

The iNGENIOUS vision: IoT Solution Providers (Section 4)

Product offering

1. What product are you offering?

   Short answer

2. Why do you think this product/service is needed?

   Answer

3. How is it different than what is already out there?

   Answer

4. What type of IoT technology is your product based on?

   - ○ *5G-based solutions*
   - ○ *NB-IoT*
   - ○ *LoRA*
   - ○ *Sigfox*
   - ○ *Others*

5. Have you developed such technologies (or prototypes) already?

   - ○ *Yes*
   - ○ *No*

6. Which is the current level of maturity of your product?

	1	*2*	*3*	*4*	*5*	
Very low	○	○	○	○	○	*Very high*

7. When do you expect a general adoption of your products?

   - ○ *Already adopted*
   - ○ *Less than 1 year*
   - ○ *1-2 years*
   - ○ *2-5 years*
   - ○ *More than 5 years*
   - ○ *Never*

Co-funded by the Horizon 2020 Framework Programme of the European Union

Marketing plan

8. Is the industry growing, shrinking or about the same?
    - *Growing*
    - *About the same*
    - *Shrinking*
9. Who are the potential customers?

    Answer
10. Who are your competitors?

    Answer
11. What market opportunities do you foresee when using IoT and/or 5G?

    Answer

SWOT Analysis

12. Strengths of IoT compared to other wireless/wired technologies:

    Short answer
13. Weaknesses:

    Short answer
14. Opportunities:

    Short answer
15. Threats:

    Short answer

Co-funded by the Horizon 2020 Framework Programme of the European Union