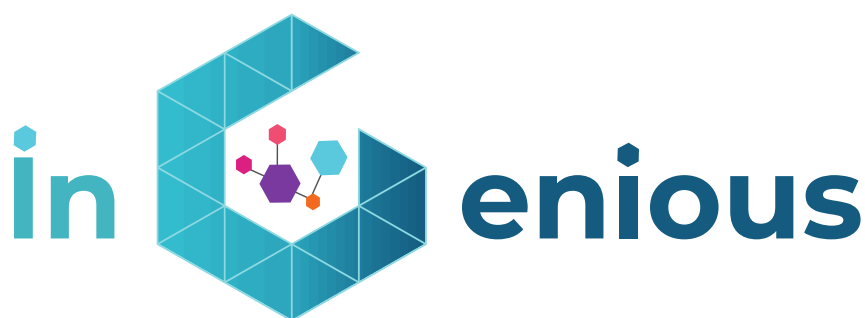




Grant Agreement No.: 957216
Call: H2020-ICT-2018-2020

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



D2.3 Regulatory Framework and Business Models

Revision: v1.0

Work package	WP2
Task	T2.3
Due date	30/11/2021
Submission date	30/11/2021
Deliverable lead	Fivecomm (5CMM)
Version	1.0
Editors	Manuel Fuentes (5CMM), Miguel Cantero (5CMM)
Authors	Manuel Fuentes (5CMM), Miguel Cantero (5CMM), Héctor Donat (5CMM), Teresa Pardo (5CMM), Stefan Köpsell (BI), Gennaro Pastore (TEI), Salvatore Esposito (TEI), Cosimo Zotti (TEI), Cristina Escribano (NOK), Efstathios Katranaras (SEQ), Julián Campo (ASTI), Luis Cascajar (ASTI), Marek Bednarczyk (PJATK), Tadeusz Puzniakowski (PJATK), Alexandr Tardo (CNIT), José Luis Cárcel (FV), Joan Meseguer (FV), Carla San Miguel (COSSP), Chiara Iorfida (COSSP), Rajesh Suseelan (iDR), Christos Politis (SES), Carlos Alcaide (TID), Giacomo Bernini (NXW), Erin E. Sender (NXW), José Costa-Requena (CMC), Ivo Bizon (TUD), Ahmad Nimr (TUD).
Reviewers	Nuria Molner (UPV), Carsten Weinhold (BI), Gennaro Pastore (TEI), Salvatore Esposito (TEI), José Luis Cárcel (FV).

Abstract	The present document describes the regulatory framework and business models related to the INGENIOUS project. The regulatory framework has been approached from different perspectives. The document discusses the spectrum issues and frequency bands available in the regions where the use cases are taking place. It also describes the requirements and limitations at network level, security and privacy concerns, cryptocurrency aspects, as well as data protection issues. The deliverable also identifies and explores the current business models at strategic level that could be derived from the iNGENIOUS results. The document first provides a PESTEL analysis for providing context, and then tackles the technological enablers that may bring to the consortium new business models and opportunities. D2.3 also describes both regulatory and business aspects concerning each of the six use cases of INGENIOUS.
Keywords	Regulatory framework, business models, spectrum, network deployment, security, privacy, cryptocurrencies, technology enablers

Document Revision History

Version	Date	Description of change	List of contributors
V1.0	30/11/2021	Public version	Manuel Fuentes (5CMM), Miguel Cantero (5CMM)

Disclaimer

This iNGENIOUS D2.3 deliverable is not yet approved nor rejected, neither financially nor content-wise by the European Commission. The approval/rejection decision of work and resources will take place at the Mid-Term Review Meeting planned in June 2022, after the monitoring process involving experts has come to an end.

The information, documentation and figures available in this deliverable are written by the "Next-Generation IoT solutions for the universal supply chain" (iNGENIOUS) project's consortium under EC grant agreement 957216 and do not necessarily reflect the views of the European Commission.

The European Commission is not liable for any use that may be made of the information contained herein.

Copyright notice

© 2020 - 2023 iNGENIOUS Consortium

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.



Executive Summary

This deliverable describes the regulatory framework and presents a first view of the business models related to the iNGENIOUS project. The document compiles information related to operational and business aspects from local, national and EU perspectives, ensuring specifically that the project propositions are compliant with the context in different supply chain domains. This is key for demonstrating the proposed use cases in real scenarios.

The regulatory framework of iNGENIOUS is herein approached from different perspectives. Spectrum issues such as the type of licensing to be used depending on the technology (licensed, unlicensed) or spectrum sharing, are discussed. The document also defines the frequency bands available in the regions where the use cases are taking place. Other aspects such as regulatory requirements and limitations at network level are presented. The document not only tackles network aspects, but also focuses on security and privacy concerns, as well as on data protection issues. The use of cryptocurrencies as part of the project, whose regulation is continuously and actively changing, is additionally analysed.

The deliverable also identifies and explores the current business models at strategic level that could be derived from the iNGENIOUS results. This is done by discussing economic concerns (how the project results are sustainable and create value); component considerations (how business is done) and strategic outcomes (design of key interdependent systems that create and sustain a competitive business). To provide some context, the document first provides a PESTEL analysis, and later discusses the technology enablers that may bring to the consortium new business models and opportunities.

The current document not only analyses the current regulatory framework and business models around iNGENIOUS from a generic perspective. It also describes both regulatory and business aspects concerning each of the six use cases in iNGENIOUS. This will permit the partners involved to better fit their needs and understand the framework where their products and services may be deployed.



Table of Contents

Executive Summary	3
List of Figures	5
List of Tables	6
Abbreviations	7
1 Introduction	9
1.1 Objectives	9
1.2 Structure.....	10
2 Regulatory Framework	11
2.1 Spectrum	11
2.2 Network Deployment: Requirements and Limitations	21
2.3 Security.....	23
2.4 Privacy and Data Protection.....	25
2.5 Use of cryptocurrencies	30
2.6 Regulatory Framework per Use Case	32
3 Business Models	36
3.1 PESTEL Analysis.....	36
3.2 Technology Enablers	43
3.3 Business Models per Use Case	50
4 Conclusion	57
4.1 Regulatory Framework	57
4.2 Business Models.....	58
Annex A: Checklist for personal data	59
References	61



List of Figures

FIGURE 1. LICENSED SHARED ACCESS ARCHITECTURE [6].	13
FIGURE 2. LORA WORLDWIDE OPERATION IN FREQUENCY BANDS PER REGION.....	18
FIGURE 3. SUBJECTS INVOLVED IN DATA TREATMENT.	27
FIGURE 4. RISK MANAGEMENT PROCESS.....	28
FIGURE 5. PRIVACY AND DATA PROTECTION WORKFLOW FOR INGENIOUS. 30	
FIGURE 6. EU MEMBER STATES DIVIDED INTO MONARCHIES AND REPUBLICS. 37	
FIGURE 7. GROSS DOMESTIC PRODUCT (GDP) EVOLUTION IN BILLIONS OF EUROS [52].	38
FIGURE 8. PESTEL IMPACT FOR INGENIOUS.....	43
FIGURE 9. NSM-AF FUNCTIONALITY IMPLEMENTATION AT THE 5GC.	47



List of Tables

TABLE 1. 5G FREQUENCIES IN FR1 (< 6 GHZ). MOST COMMON FREQUENCIES ARE HIGHLIGHTED.	15
TABLE 2. 5G FREQUENCIES FOR FR2 (> 6 GHZ).	15
TABLE 3. FREQUENCY BANDS USED BY SATELLITE.	17
TABLE 4. LORA FREQUENCY BAND, BANDWIDTH, AND DATA RATES PER REGION.	18
TABLE 5. FREQUENCY ALLOCATION IN SPAIN.	19
TABLE 6. FREQUENCY ALLOCATION IN ITALY.	20
TABLE 7. POWER TRANSMISSION LEVEL RESTRICTIONS IN SPAIN.	23
TABLE 8. REGULATORY FRAMEWORK OF THE AUTOMATED ROBOTS WITH HETEROGENEOUS NETWORKS UC.	32
TABLE 9. REGULATORY FRAMEWORK OF THE TRANSPORTATION PLATFORM HEALTH MONITORING UC.	34
TABLE 10. REGULATORY FRAMEWORK OF THE INTER-MODAL ASSET TRACKING VIA IOT AND SATELLITE UC.	34
TABLE 11. REGULATORY FRAMEWORK OF THE SITUATIONAL UNDERSTANDING AND PREDICTIVE MODELS IN SMART LOGISTICS SCENARIOS UC.	35
TABLE 12. REGULATORY FRAMEWORK OF THE SUPPLY CHAIN ECOSYSTEM INTEGRATION UC.	35
TABLE 13. POLITICAL FACTORS AROUND THE INGENIOUS PROJECT.	38
TABLE 14. CURRENT CURRENCIES USED IN EU MEMBER STATES.	39
TABLE 15. ECONOMIC FACTORS AROUND THE INGENIOUS PROJECT.	39
TABLE 16. SOCIAL FACTORS AROUND THE INGENIOUS PROJECT.	40
TABLE 17. TECHNOLOGICAL FACTORS AROUND THE INGENIOUS PROJECT. .	41
TABLE 18. ENVIRONMENTAL FACTORS AROUND THE INGENIOUS PROJECT. 	42
TABLE 19. LEGAL FACTORS AROUND THE INGENIOUS PROJECT.	42
TABLE 20. BUSINESS MODEL CANVAS OF THE AUTOMATED ROBOTS WITH HETEROGENEOUS NETWORKS UC.	51
TABLE 21. BUSINESS MODEL CANVAS FOR THE IMPROVE DRIVERS’ SAFETY WITH MR AND HAPTIC SOLUTIONS UC.	51
TABLE 22. BUSINESS MODEL CANVAS FOR THE TRANSPORTATION PLATFORM HEALTH MONITORING UC.	52
TABLE 23. BUSINESS MODEL CANVAS FOR THE INTER-MODAL ASSET TRACKING VIA IOT AND SATELLITE UC.	53
TABLE 24. BUSINESS MODEL CANVAS FOR THE SITUATIONAL UNDERSTANDING AND PREDICTIVE MODELS IN SMART LOGISTICS SCENARIOS UC.	55
TABLE 25. BUSINESS MODEL CANVAS FOR THE SUPPLY CHAIN ECOSYSTEM INTEGRATION UC.	56
TABLE 26. GDPR CHECKLIST FOR PERSONAL DATA.	59



Abbreviations

3GPP	Third Generation Partnership Project
4G	Fourth Generation
5G	Fifth Generation
5GPPP	The 5G infrastructure Public Private Partnership
ALKS	Automated Lane Keeping Systems
ARPA	<i>Agenzia Regionale per la Protezione Ambientale</i>
ATEX	<i>Appareils destinés à être utilisés en ATmosphères Explosives</i>
BPSK	Binary Phase-Shift Keying
CAG	Closed Access Group
CAGR	Compound Annual Growth Rate
CBDC	Central Bank Digital Currency
CEPT	European Conference of Posts and Telecommunications
CJEU	Court of Justice of the European Union
CNAF	<i>Cuadro Nacional de Atribución de Frecuencias</i>
CSIRT	Computer Security Incident Response Team
CSP	Communication Service Providers
DLT	Distributed Ledger Technology
DPO	Data Protection Officer
ECB	European Central Bank
EIRP	Effective Isotropic Radiated Power
eMBB	Enhanced Mobile Broadband
ESV	Earth Stations on Vessels
ETSI	European Telecommunications Standards Institute
EU	European Union
E-UTRA	Evolved UMTS Terrestrial Radio Access Network
FR	Frequency Range
FTC	Federal Trade Commerce
GDP	Gross Domestic Product
GDPR	General Data Protection Regulation
GFSK	Gaussian Frequency Shift Keying
GSM	Global System for Mobile Communications
ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IMT	International Mobile Communications
IoT	Internet of Things
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centres
ISM	Industrial Scientific and Medical
ISO	International Organization for Standardization



ITU	International Telecommunication Union
ITU-R	ITU Radiocommunication Sector
ITU-T	ITU Telecommunication Standardization Sector
LAN	Local Area Network
LoRa	Long Range
LoRaWAN	Long Range Wide Area Network
LPWAN	Low Power Wide Area Network
LSA	Licensed Shared Access
LTE	Long Term Evolution
LTE-M	Long Term Evolution for Machines
MFCN	Mobile/Fixed Communications Networks
MNO	Mobile Network Operator
MSS	Mobile Satellite Services
NB-IoT	Narrowband Internet of Things
NIS	Network and Information Security
NPN	Non-Public Network
NR	New Radio
OA&M	Operations, Administration and Management
OASIS	Outcome and Assessment Information Set
PDU	Power Distribution Unit
PESTEL	Political-Economical-Social-Technological-Environmental-Legal
PLMN	Public Lan Mobile Network
PNI-NPN	Public Network Integrated NPN
PNRF	<i>Piano Nazionale di Ripartizione delle Frequenze</i>
QoS	Quality of Service
R&D	Research and Development
RAN	Radio Access Network
RSPG	Radio Spectrum Policy Group
SBA	Service-Based Arquitechture
SCIA	Start of Activities Certified Notification
SDO	Standards Development Organisation
ToD	Tele-operated Driving
TSN	Time Sensitive Networking
UHF	Ultra High Frequency
UK	United Kingdom
UMTS	Universal Mobile Telecommunications System
URLLC	Ultra Reliable Low Latency Communication
US	United States
USD	US Dollar
VAT	Value Added Tax
WRC	World Radiocommunication Conference



1 Introduction

This deliverable is the first report related to the Task 2.3 of the iNGENIOUS project. D2.3 mainly aims at capturing the current status (as of November 2021) of the regulatory matters and potential business models that could be derived from the project. The following section describes the main objectives of the project concerning both aspects.

1.1 Objectives

Regulation is a key aspect when talking about implementation procedures, as processes may be limited somehow or regulated to follow a specific directive. This is usually done by authority entities or regulation bodies at European, national, or local levels. Depending on the case to study, authorities may take part in the regulation process. In such case, the highest authority takes the priority. The relevance and impact of a particular area of regulation depends on the type of use case and technology deployment.

This deliverable discusses in detail the different regulation aspects that affect the iNGENIOUS project, not only from a general perspective, but also from a use case point of view. To do so, first some general aspects that directly affect the deployment and validation of the use cases are described. Naturally, spectrum issues such as the type of licensing, tightly related to the technology deployment, is a key aspect to keep in mind.

However, regulation is not only about available spectrum. There are many other aspects that need to be considered when deploying a particular technology. Network aspects including maximum transmission powers is a key aspect to analyse when deploying communication networks. Security and privacy are crucial for guaranteeing a specific service to the end users. Additionally, regulation in a novel domain such as cryptocurrencies needs to be explored. All these aspects are herein considered and described in detail.

The document provides details about the regulatory framework surrounding each one of the six use cases. The following aspects have been considered:

- *Automated Robots with Heterogeneous Networks*: functional safety in AGVs and robots, spectrum.
- *Improve Drivers' Safety with MR and Haptic Solutions*: spectrum, automated lane-keeping systems regulation.
- *Transportation Platform Health Monitoring*: safety, fire and explosions, spectrum, security, data protection and privacy.
- *Inter-modal Asset Tracking via IoT and Satellite*: spectrum, data protection and privacy, security.
- *Situational Understanding and Predictive Models in Smart Logistics Scenarios*: spectrum, data protection and privacy, security.
- *Supply chain ecosystem integration*: data protection and privacy.

Besides technology maturity, viable business cases are essential for deployment and evolution of the envisaged use cases. The use of next generation IoT technologies in the considered use cases and scenarios may 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 operative. iNGENIOUS will bring to such players the necessary tools to further develop their business opportunities.

As done with the regulatory framework, business models that can be derived specifically from each one of the use cases are analysed. This has been done by providing a complete business model canvas per use case with the following information: key partners, activities, resources, value propositions, customer relationships, channels to reach customers, customer segment, costs, and revenues.

1.2 Structure

The document is structured in two main chapters, each describing one of the aforementioned fields.

- **Chapter 2 (Regulatory Framework)** describes spectrum licensing alternatives, available frequency bands, security aspects, privacy and data protection concerns, the use of cryptocurrencies, and the specific use case regulations.
- **Chapter 3 (Business Models)** provides a complete PESTEL (Political-Economical-Social-Technological-Environmental-Legal) analysis evaluating the context of iNGENIOUS. Additionally, it also discusses some of the main technologies that would enable new business models and opportunities.

Finally, the main findings of this deliverable regarding these two fields are provided in **Chapter 4 (Conclusion)**.



2 Regulatory Framework

The following chapter describes the regulatory aspects affecting the deployment and validation of real scenarios in iNGENIOUS.

2.1 Spectrum

The directives of spectrum for telecommunication systems (including IoT through industrial and satellite networks, among others) are mainly covered by the International Telecommunication Union (ITU), the regulatory body specialised in defining directives for information and communication technologies. Its Radiocommunication Sector (ITU-R) is responsible for radio communication aspects such as managing the international radio-frequency spectrum, while its Telecommunication Standardisation Sector (ITU-T) develops international standards (known as ITU-T recommendations) for defining the global infrastructure of Information and Communication Technologies (ICT).

ITU also sets the requirements for every communication generation. For instance, the ITU-R recommendation M.2083-0 [1] describes the framework and the overall objectives of the future development of International Mobile Telecommunications (IMT) systems for 2020 and beyond.

In the following sections, the document discusses the types of licensing when acquiring spectrum for the technologies envisaged in iNGENIOUS, as well as the available frequencies that have been addressed to such technologies.

2.1.1 SPECTRUM LICENSING

Spectrum is a scarce resource with limited nature and availability, Interferences may be caused when several users try to access the same portion of a frequency range. For this reason, spectrum is highly regulated in the world.

The spectrum used for mobile communications (from MHz to GHz) is divided in ranges and slots, being some slots public and others private. The public spectrum is the one everybody can radiate without any legal restriction in terms of frequency (not in other terms, like power), while the private one requires a license agreement. Such licenses can be organised in numerous ways and are handled by an authority in the territory. The different types of spectrum licensing methods are explained in the following subsections.

2.1.1.1 Licensed spectrum

Licensed spectrum is defined as the portion of radio spectrum that is designated by international, national, or local regulators to be reserved for organizations with granted licenses (e.g., mobile/satellite operators and verticals). Technologies such as 5G, NB-IoT or satellite communications are associated to this type of licensing. This type of licensing is also related to the use of Non-Public Networks (NPN), where private spectrum is used by licensees different from operators but under the same type of regulation.



There are two spectrum right types: property and common rights. The property one stands for regular licensing, where the regulator body grants licenses to private companies for the exploitation of the spectrum. On the other hand, the common rights can be created either by the regulatory body or by a licensee, and this is what we call spectrum sharing. This is further discussed in Section 2.1.1.2.

Licensed spectrum can be in turn:

- **Permanent:** permits regular access to spectrum by the licensee.
- **Temporary** (also known as spectrum leasing): spectrum is reserved for a specific event or service.

Naturally, acquiring either a permanent or temporary license for using a specific service brings a series of advantages to the license holder, such as the rights to be the only one using a specific frequency range in a particular region. However, it may also bring some inflexibility and restrictions in transmission power or accessibility.

One of the most important organisations that develops standards traditionally using licensed spectrum¹ for mobile telecommunications systems based on cellular technologies is the Third Generation Partnership Project (3GPP). This organisation unites Standard Development Organisations (SDOs) from around the world and provides its members with a stable environment to produce the reports and specifications that define 3GPP technologies. 3GPP technologies are developed following the requirements from ITU and are designed to operate in the IMT bands identified by ITU-R.

As for 5G NR, E-UTRA and UTRA (with the latter two being the radio interface technologies of LTE and UMTS, respectively) 3GPP has defined the operating bands in specifications [2], [3], [4]. So far, 3GPP has specified more than 70 frequency bands for NR and LTE within the IMT bands in specific national or regional areas.

2.1.1.2 Spectrum sharing

As it has been set, the lack of spectrum is one of the main problems when talking about cellular communications. Nowadays, finding completely clear bands for the use of mobile communications is sometimes a hard task, and spectrum sharing could be a solution to use spectrum bands when they are not being used in some areas and/or time slots.

When using spectrum sharing, it is possible to use a specific service that is created either by the regulatory body or by a licensee. A private entity that has the rights of a band can establish its own operating rules and allow devices to use its spectrum.

The traditional model of Licensed Shared Access (LSA) was developed in Europe for the 2.3 GHz band, and now there are advanced models being developed in [5]. A simple architecture of LSA is shown in Figure 1 [6]. The incumbents are the owners that share the spectrum under a sharing

¹ Technologies developed by 3GPP can also be now deployed in unlicensed spectrum, leveraging the work done for instance in context of LTE and NR for Unlicensed spectrum (LTE-U and NR-U, respectively).



agreement. Any stakeholder will need to negotiate the LSA Repository before any usage. The LSA Repository is a database with information such as availability, protection zones or requests for LSA bands from the incumbents. The LSA controller processes the information from the LSA repository to identify spectrum opportunities. The Operations, Administration and Management (OA&M) interacts with the LSA controller and authorises the access to the LSA bands.

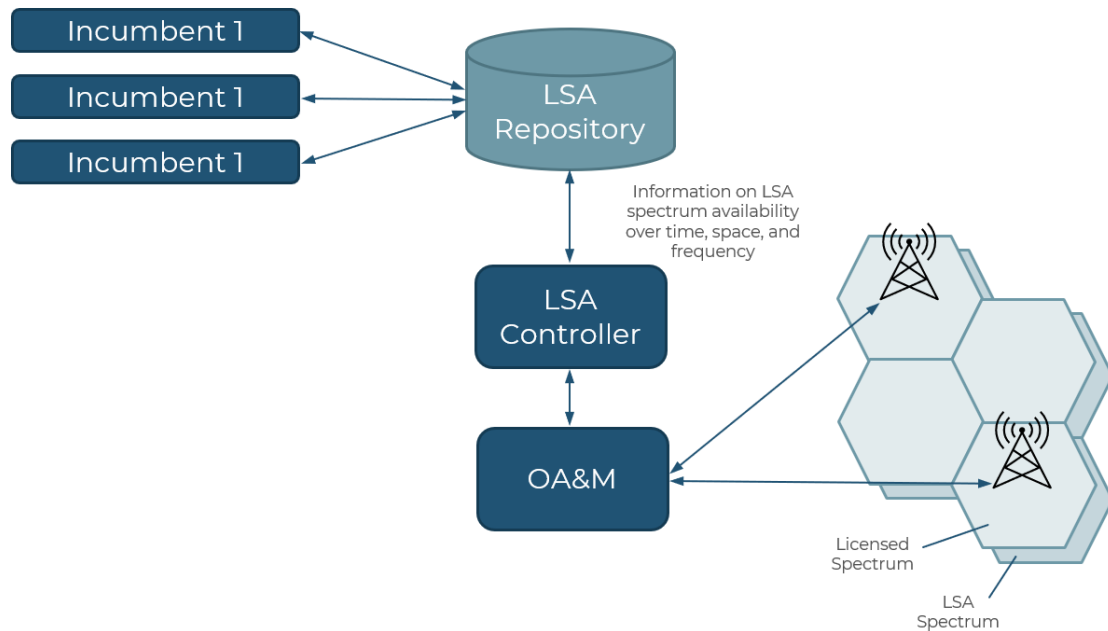


Figure 1. Licensed shared access architecture [6].

In 5G, spectrum sharing can play an important role if it enables new bands that otherwise would not be available. A careful planning is needed for success, as a unoptimized sharing framework could limit the potential impeding 5G deployments or imposing power restrictions.

2.1.1.3 Unlicensed spectrum

Unlicensed spectrum encompasses the set of frequency bands assigned to every citizen for non-exclusive usage, thus avoiding regulatory constraints, which are often introduced and controlled by regulatory bodies. To access unlicensed frequency bands, users just need to use equipment that corresponds to certain established technical standards such as Wi-Fi or Bluetooth².

Unlicensed spectrum bands are irregularly distributed across both sub-6GHz and above 6GHz bands worldwide:

- **Below 6 GHz:** few frequency bands are available for unlicensed spectrum due to spectrum scarcity caused by the licensing of low frequency bands, which are more prone to cause interference due to its long signal propagation properties. Typically, the 2.4 GHz, also known as Industrial, Scientific, and Medical (ISM) band, and 5 GHz spectrum

² In response, 5G radio frequency ranges now include all those previously held by 4G, as well as more frequencies up to 6GHz (Sub-6) and the high band mm-Wave spectrums.



bands are the main unlicensed bands worldwide, being used for technologies such as Wi-Fi and Bluetooth. Additionally, the 5.2 – 5.7 GHz band is already available for the operation of 5G NR in unlicensed bands (5G NR-U) [7].

- **Above 6 GHz:** the expansion of 5G capabilities to operate in mm-wave frequencies has opened the door for exploiting the huge potential of unlicensed spectrum in high frequency bands. In addition, the Sub-6 capacity could theoretically run out in mature markets by 2023 as a direct result of the rise in data consumption. This would effectively make 5G mm-wave a valuable resource for the continued offering of enhanced mobile broadband services. Until the auction of 26 GHz band, this band has been considered in different countries as a good option for performing unlicensed spectrum operation. In the future, 37-50 GHz and 64-71 GHz are seen as the main candidates for enabling unlicensed spectrum operation for beyond 5G and IoT technologies [7].

In all frequency ranges, free access to unlicensed spectrum bands offers at the same time a large set of opportunities - thanks to the non-dependence on operators - and limitations, mainly related to the congestion and interferences caused by the uncoordinated access of multiple users to a non-regulated medium without transmission power restrictions.

As a consequence, within IoT and 5G technologies, unlicensed spectrum is seen as a complementary solution for enabling the delivery of 5G across a range of different spectrum bands. In these conditions, unlicensed spectrum allows any organisation to roll out 5G networks without needing to apply for a spectrum licence, especially for use locally indoors. This aspect is called to meet the need for deploying local private 5G networks in industrial scenarios such as maritime ports or factories, without the need of a network operator. Alternatively, unlicensed spectrum may also help operators to augment the 5G user experience by aggregating licensed and unlicensed bands to support faster services [8].

2.1.2 FREQUENCY BANDS

The current section describes the frequency bands that are/will be available for use case demonstration. This exercise has been done from two perspectives. First, the frequency bands available per technology are analysed, which have been assigned by international regulators. Later on, the specific bands available per region are described. This is done for the two countries where the iNGENIOUS trials will take place, i.e., Italy and Spain.

2.1.2.1 Frequencies per technology

5G New Radio

By the end of 2017, 3GPP approved the first 5G NR radio specifications [9]. In TS 38.101 [10], 3GPP defined two Frequency Ranges (FRs) for 5G NR operation:

- **FR1:** 450–6000 MHz (including low- and mid-band).
- **FR2:** 24250–52600 MHz (mm-wave range).



The frequency bands for 5G wireless technology are classified into FR1 and FR2 frequency ranges. FR1 (4.1 GHz to 7.125 GHz) band of frequencies are used for carrying most of the traditional cellular mobile communications traffic, while the FR2 (24.25 GHz to 52.6 GHz) band of frequencies are focused on short-range, high data rate capabilities. The lists of operating bands in respective FRs contain both newly identified bands for NR (e.g., n77, n78, n257, n258, n260) as well as reused LTE bands (e.g., n1, n2).

The following Table 1 shows a summary of the frequencies available for 5G in sub-6GHz band, while Table 2 provides the bands for mm-wave. The complete range of frequencies for 5G can be found in [10].

Table 1. 5G frequencies in FR1 (< 6 GHz). Most common frequencies are highlighted.

Band	Mode	UL	DL
n1	FDD	1920 MHz – 1980 MHz	2110 MHz – 2170 MHz
n2	FDD	1850 MHz – 1910 MHz	1930 MHz – 1990 MHz
...			
n38	TDD	2570 MHz – 2620 MHz	2570 MHz – 2620 MHz
n39	TDD	1880 MHz – 1920 MHz	1880 MHz – 1920 MHz
n40	TDD	2300 MHz – 2400 MHz	2300 MHz – 2400 MHz
n41	TDD	2496 MHz – 2690 MHz	2496 MHz – 2690 MHz
n46	TDD	5150 MHz – 5925 MHz	5150 MHz – 5925 MHz
...			
n77	TDD	3300 MHz – 4200 MHz	3300 MHz - 4200 MHz
n78	TDD	3300 MHz - 3800 MHz	3300 MHz - 3800 MHz
n79	TDD	4400 MHz - 5000 MHz	4400 MHz - 5000 MHz
...			
n96	TDD	5925 MHz - 7125 MHz	5925 MHz - 7125 MHz
n97	SUL	2300 MHz - 2400 MHz	N/A
n98	SUL	4400 MHz - 1920 MHz	N/A

Table 2. 5G frequencies for FR2 (> 6 GHz).

Band	Mode	UL	DL
n257	TDD	26500 MHz - 29500 MHz	26500 MHz - 29500 MHz
n258	TDD	24250 MHz - 27500 MHz	24250 MHz - 27500 MHz
n259	TDD	39500 MHz - 43500 MHz	39500 MHz - 43500 MHz
n260	TDD	37000 MHz - 40000 MHz	37000 MHz - 40000 MHz
n261	TDD	275000 MHz - 28350 MHz	27500 MHz - 283500 MHz



Industrial IoT

A key factor for the endorsement of wireless solutions for industrial networks has to do with the licensed spectrum for such purposes that is handled, since high availability and reliability is needed [11]. Generally, there are countries that provide local dedicated spectrum for industrial usage (e.g., Germany in 3700-3800 MHz and Japan in the 28 GHz band) to deploy private networks. On the other hand, there are also countries (e.g., France or Italy) that only allocate spectrum to communication service providers. Thus, an option here is to obtain spectrum indirectly from the national regulator, that is, sub-leasing from an existing mobile network operator. Tables 1 and 2 in [11] summarise the spectrum allocations and regulatory discussions on assignment of spectrum dedicated to industrial applications as of April 2021.

Since 2018, 3GPP has been performing studies and normative work for the development of technologies relevant to Industrial IoT (IIoT) technologies. More specifically, as part of a set of studies for 5G enhanced support of vertical and Local Area Network (LAN) services, 3GPP SA groups studied the feasibility on vertical LANs [12], as well as network management enhancements required to support NPN management [13].

Moreover, a RAN study on NR Industrial Internet of Things (NR IIoT) started in Release 16 [14] and the standardisation work will be further completed in Release 17. This new communication class aims to cover industrial applications related to factory automation (i.e., logistics, sensor networks, robotics, and augmented reality) where both eMBB and URLLC features become vital elements to support high transmission reliability and performance

TSN is also a key enabler for NR IIoT. It encompasses a set of standards identified by the IEEE 802 family that enables Ethernet wired networks to ensure Quality of Service (QoS) features for time-sensitive traffic and critical-data applications, to provide deterministic transmissions by synchronizing various equipment components to a single master clock [15]. In TSN, it is not necessary to use the internet protocol since Ethernet frames can be transported over the 5G system in an Ethernet Power Distribution Unit (PDU) session type. Mechanisms to ensure deterministic delays and synchronisation were defined by IEEE and the objective of 3GPP was to adapt these mechanisms to the wireless and 5G world.

Satellite communications

Satellite is a wireless communication infrastructure providing broadcast, broadband and interactive services using frequencies that are part of the electromagnetic spectrum. Most are shared with terrestrial wireless systems. The ITU has allocated parts of this spectrum range to specific categories of services and has identified those frequencies best suited for transmissions via satellite. While some bands are exclusively dedicated to satellite transmission, most are shared with terrestrial wireless services. As satellites transmit concurrently across borders and continents, instantly establishing connections over thousands of kilometres, the identified frequencies must also be available concurrently across the whole satellite footprint. Overall, satellite is one of many users of radio spectrum.



Different frequency bands are suitable for different types of markets as shown below. Lower frequencies (L-, S- and C-Bands) are less affected by the heavy rainfall in parts of Africa/Asia/Latin America and can serve wide areas of the globe at a time. Higher frequencies (Ku-, Ka- and Q/V Bands) allow smaller antennas to be used with more focused service beams on regions or sub-regional areas. Such frequency bands are shown in Table 3.

Table 3. Frequency bands used by satellite³.

Band	Frequencies	Applications and Services
S-DAB	1.467 - 1.492 GHz	Satellite Audio Broadcasting to fixed/mobile units.
L-Band	1.518 - 1.675 GHz	Civilian Mobile-Satellite Services (two-way).
S-Band	1.97 - 2.69 GHz	Satellite television, radio broadcasting and mobile BB services including in-flight connectivity.
C-Band	3.4 - 7.025 GHz	Fixed-Satellite television and data services (including broadcasting).
Ku-Band	10.7 - 14.5 GHz	Fixed-Satellite television and data services (including broadcasting).
Ka-Band	17.3 - 30 GHz	Fixed-Satellite television and data services including fixed/mobile two-way broadband.
Q/V-Bands	37.5 - 51.4 GHz	Fixed and mobile high-speed broadband services including in-flight connectivity.

Generally, the potentially wide multi-country coverage of satellite radio systems is a challenge when it comes to fulfilling regulatory requirements [16]. Here, it should be noted that there is no restriction on what frequency bands to be used in IoT-over-satellite communications.

From 3GPP side, in 2019, SA1 work group approved a new Rel-18 study to address aspects related to extra-territorial coverage of satellites and high-altitude systems. Current terrestrial 3GPP systems are typically deployed so that they provide coverage within a single country only, fulfilling the associated regulatory obligations for that specific country. Satellite-based radio systems may, however, cover multiple countries or cover international waters. This leads to new challenges for the 3GPP system. The study [17] aims to study use cases of extra-territoriality, identify relevant features, technical aspects, and applicable types of regulations; the ongoing relevant work is documented in TR 22.926 [18].

Sigfox and LoRa

The low power, long range and long battery life capabilities required by new IoT applications also contributed to the adoption of different non-3GPP technologies in the segment of Low Power Wide Area Networks (LPWAN). Among existing LPWAN technologies, LoRa and Sigfox are the two most popular solutions leveraging unlicensed spectrum access.

Sigfox is an ultra-narrowband and low power IoT technology designed to transmit short volumes of data in large coverage ranges while keeping low

³ UHF (235 to 400 MHz) and X-band (7250-8400 MHz) are also used for military services.



cost and long battery life capabilities. Sigfox transmits non-periodic small data volumes (12 bytes) from sensors and devices by exploiting Binary Phase-Shift Keying (BPSK) and Gaussian Frequency Shift Keying (GFSK) modulations in tiny slices of unlicensed spectrum of 100 Hz within 868-869 MHz frequency band in Europe and 902-928 MHz in US. The maximum data rate provided by Sigfox in this reduced spectrum is around 100 bps.

LoRaWAN (Long Range Wide Area Network Protocol) is a LPWAN solution designed to enable low range communications while keeping low-cost and low-power consumption over unlicensed spectrum to billions of IoT devices. LoRa relies on chirp spread modulation (SS Chirp) that allows to maintain low power characteristics while increasing the communication range. To enable long range coverage, this feature is combined with an unlicensed spectrum operation in channels of 125/500 kHz wide (depending on the region and the frequency band) below 1 GHz. LoRaWAN operates in a wider amount of spectrum than SigFox and therefore, gets more interferences due to its presence in unlicensed bands. Depending on the region, LoRaWAN operates in different unlicensed spectrum bands as shown in Figure 2.

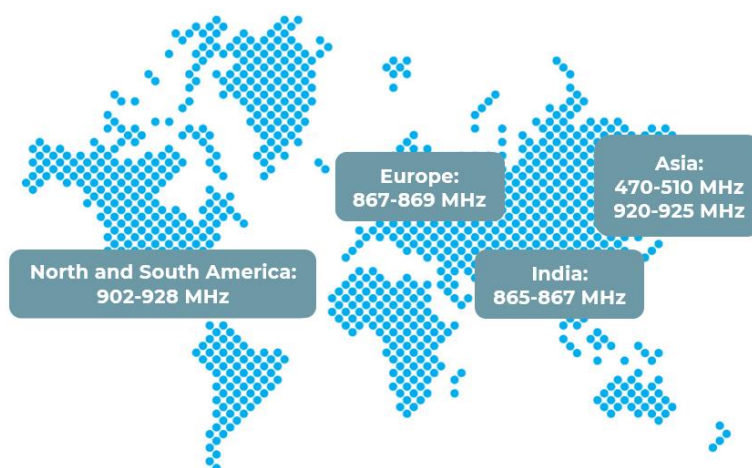


Figure 2. LoRa worldwide operation in frequency bands per region.

The channel bandwidth and data rates transmitted in each region are shown in Table 4.

Table 4. LoRa frequency band, bandwidth, and data rates per region.

	Europe	North and South America	Asia	India
Frequency band	867-869 MHz	902-928 MHz	470-510 MHz 920-925 MHz	865-867 MHz
Channels	10	64 + 8 + 8	In definition by Technical Committee	In definition by Technical Committee
Channel BW	125 kHz	500 kHz		
Data rate	250 bps – 50 kbps	980 bps – 21.9 kbps		



2.1.2.2 Frequencies per region

As it has been explained, the fact that specific frequency bands are assigned to a technology, does not always mean that they can be used. This will also depend on local and national regulators, which assign the frequencies to be used within all possible ones assigned to a technology. This section discusses in detail the potential frequencies to be used, for the iNGENIOUS considered technologies in Europe, as well as in the two countries where the trials are taking place, i.e., Spain and Italy.

Europe

The IMT spectrum for cellular technologies per region is harmonised in ITU-R. In Europe, the spectrum considered for 5G includes three bands:

- 703–788 MHz (for low-band).
- 3.4–3.8 GHz (for mid-band).
- 24.25–27.5 GHz (for mm-wave).

The 3.4–3.8 GHz band was considered by the Radio Spectrum Policy Group (RSPG), a high-level advisory group that assists the EC in the development of radio spectrum policy, as *“the primary band suitable for the introduction of 5G-based services in Europe even before 2020 given that it is already harmonized for mobile networks and offers wide channel bandwidths”* [19].

According to RSPG, *“5G will need to be deployed also in bands already harmonized below 1 GHz, including particularly the 700 MHz band, in order to enable nation-wide and indoor 5G coverage.”* Note that the 703–733 MHz uplink / 758–788 MHz downlink band has already been auctioned in some countries, e.g., in France and Germany. RSPG also recognised the 24.25–27.5 GHz (also known as '26 GHz') band *“as a pioneer band for Europe to be harmonized before 2020.”*

Spain

In Spain, the National Table of Frequency Allocation (CNAF) [20] is the entity that regulates the use of the spectrum in a national context, following the ITU regulations and recommendations, for all frequencies between 8.3 kHz and 3000 GHz. Table 5 shows a summary of the main low- and mid-frequency bands assigned to different technologies.

Table 5. Frequency allocation in Spain.

Frequency band (MHz)	Service
87.5 – 108	FM audio broadcasting
470 – 694	Television broadcasting Terrestrial mobile
694 – 790	Television broadcasting
790 – 890	Cellular technologies (mobile phones) Fixed devices (Wireless microphones, RFID, PMSE, etc.)
890 – 915 925 – 960 1715 – 1785 1810 – 1880	Cellular technologies (mobile phones)



1980 – 2010	Mobile Satellite Services (MSS)
2500– 2690	Cellular technologies (mobile phones)
3400 – 3800	Cellular technologies (mobile phones) Satellite links (space - earth) Mobile/Fixed Communications Networks (MFCN)

Note that CNAF was approved by the Spanish government in October 2017, and modified later in April 2018 and July 2020. It was firstly published in 1990, but it requires constant updates from the international regulatory bodies, more concretely the ITU, the European Conference of Posts and Telecommunications (CEPT), the European Union (EU) and the European Telecommunications Standards Institute (ETSI). These regulatory bodies approve regulations, take decisions, and make recommendations towards spectrum harmonisation.

A reorganisation of the spectrum has been done twice in Spain, to reduce the spectrum bands for terrestrial television and use this bands for mobile communications. This is known as the Digital Dividend. The first reallocation of spectrum was done in 2014-2015, where the 800 MHz band used for digital TV was assigned to 4G LTE services. The second reallocation was done in 2020, which objective was to use 5G NR services in the 700 MHz band, where digital TV was also placed.

Italy

In Italy, the National Frequency Distribution Plan (PNRF) regulates the use of the radio spectrum for all frequency bands between 0 and 3000 GHz (in Table 6, the main frequency bands are summarised) by attributing each band to different services and/or applications [21]. It has been approved by decree of the Minister of Economic Development dated May 27, 2015.

Table 6. Frequency allocation in Italy.

Frequency bands (MHz)	Service	Employment
87.5 – 108	Radio broadcasting	FM audio broadcasting
470 – 608	Radio broadcasting	Television broadcasting Temporary broadband audio connections
608 – 614	Radio broadcasting Radio astronomy	Television broadcasting Temporary broadband audio connections
614 – 790	Radio broadcasting	Television broadcasting Temporary broadband audio connections
790 – 862	Mobile	Terrestrial electronic communication services (mobile phones) International Mobile Telecommunications (IMT)
876 – 915 921 – 960 1715 – 1785 1810 – 1880	Mobile	GSM cellular network (Europe)
1980 – 2010	Mobile	Mobile Satellite Services (MSS)
2510 – 2600 2630 – 2690	Mobile	Terrestrial electronic communication services (mobile phones), IMT



3500 – 3800	Land line Satellite land line Mobile	Broadband and ultra-broadband terrestrial electronic communications services (Fixed Wireless Access, LTE) Mobile/Fixed Communications Networks (MFCN) Earth Stations on Vessels (ESV)
--------------------	--------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

PNRF oversees the introduction into Italian legislation of ITU-R regulations, which constitute a binding international treaty for member countries, as well as the final acts of the World Radiocommunication Conferences (WRC). Furthermore, PNRF also implements the mandatory provisions approved by the EU and (voluntarily) the CEPT recommendations.

The radioelectric spectrum planning has been subjected to important rearrangements during the legislatures, basically reducing the band assigned to television broadcasting and allocating it to emerging mobile communication standards. In 2018, the rights to use the GSM (900 MHz band) and UMTS (1800 MHz) frequencies for mobile communications were renewed to encourage the development of 4G LTE technologies that can work on different bands, including the 800 MHz band previously occupied by television channels.

NB-IoT is based on a cellular network architecture and exploits the existing commercial LTE infrastructure, after a software update of the radio base stations, using the related licensed radio bands [22]. In addition, the Budget Law for 2018 established the procedures for assigning the frequency bands 694–790 MHz, 3.6–3.8 GHz and 26.5–27.5 GHz to 5G [23]. On 11 July 2018, the Ministry of Economic Development launched an auction that set off the assignment of 1275 MHz of spectrum in the 5G bands, and consequently the fulfilment of the European 5G Action Plan. The frequencies reallocation to 5G envisages the release of the UHF band (from 694 to 790 MHz) currently assigned to radio and television broadband operators starting from 1 July 2022. This will be a similar operation as the one occurred in Spain in 2020.

2.2 Network Deployment: Requirements and Limitations

The service-based architecture (SBA) defined in 5G core enables different deployments depending on frequency regulation and infrastructure owners. If the frequency is owned by a public mobile operator, it can be leased or rented to external companies to deploy their own infrastructure using that frequency. The public mobile operator that owns the frequency can also provide the network infrastructure to the company that requires private mobile network for its own business.

If the frequency is owned by the company that intends to deploy a 5G NPN, then the infrastructure deployment can also be owned by the same company. This company can utilise the 5G network for its own services but can also provide the network as a wholesale to other public operators or companies that require mobile connectivity. The concept of neutral host can be considered an extension of this deployment, where the company owns the frequency and infrastructure but re-sells network slices to other companies.



The rules governing the installation of mobile base stations are part of a complex framework of national, regional, and municipal provisions. For instance, the installation of mobile stations. Different administrative procedures are envisaged depending on the type of intervention (e.g., new fixed installation, new moving installation, or reconfiguration of an existing station), the position of the system (single structure or structure shared with another operator) and power implemented.

2.2.1 NETWORK DEPLOYMENT IN ITALY

In Italy, the installation of mobile stations is regulated by the articles 86 and following of the Legislative Decree no. 259 of 2003 [24], which ascertains compliance with the emission limits set by the Decree of the President of the Council of Ministers of 8 July 2003 [25]. In Italy, there are different procedures to obtain the authorisation to install a mobile station. In some cases, it is necessary to initiate a procedure to obtain an authorisation document by the local administration (power output between 20W and 150W); in other cases, it is possible to use simplified procedures such as the Start of Activities Certified Notification (SCIA) or the structure installation notification disclosed at the beginning of the works (power output less than 20W).

About the SCIA simplified procedure, the preliminary steps that the future manager of the new mobile station has to perform for the placement of a new fixed installation, or the reconfiguration of an existing system are the following:

- Sending of a structure installation notification to Regional Agency for the Environmental Protection (ARPA) which then responds by providing its advice regarding the radio-electric aspects of the installation.
- Sending of a technical-health report, concerning the level of the pre-existing and forecasted electromagnetic field, to the Local Health Department (*Azienda Sanitaria Locale*) that provides its advice on health aspects related to the installation of the system.
- The request for the advice of the municipal technical offices regarding the urban-landscape compatibility of the system to be installed.
- The request for any further advice and/or authorisations and/or (e.g., landscape authorisation) where required.

In case of a moving system installation, the municipal technical offices verify the compliance of the project with the regulatory requirements in addition to any ARPA prescriptions, communicating the check results to the One-stop Shop for Construction (SUED).

The practices must therefore be submitted to the municipal One-stop Shop for Productive Activities (SUAP) in order to obtain the necessary authorisations to finally proceed with the actual installation of the system.

2.2.2 NETWORK DEPLOYMENT IN SPAIN

In Spain, “*Ley 9/2014, de 9 de mayo, General de Telecomunicaciones*” [26] regulates the telecommunications framework, considering aspects such as



network deployments and an efficient use of the spectrum in the country. It has been updated several times, being the last one in October 2021.

When considering a network deployment in Spain for iNGENIOUS, it will be affected by the maximum transmission power levels. A good example is the use case on *Improve Drivers' Safety with MR and Haptic Solutions*. The given scenario consists of an AGV tele-operated through 5G in an outdoor open space in the port of Valencia, Spain. To enable this connectivity, a 5G NSA mm-wave antenna is deployed in the area and a 5G mm-wave modem is attached to the mobile AGV platform.

Since the technology to use is 5G mm-wave, in the frequency band n258, the radioelectric station parameters have been settled in the deployment in such a way that the “*Real Decreto 1066/2007*” [27] is fulfilled. This decree establishes conditions for the protection of the public radioelectric spectrum domain, restrictions on radio emissions and sanitary protection measures against radio emissions. The following table presents an example of the typical transmission levels that could be used in this case.

Table 7. Power transmission level restrictions in Spain.

Parameter	Value
Polarisation	B
Gain	29 dB
Radiated power type	EIRP
Reflection coefficient	1
Maximum power level	251.19 W
Max. azimuth radiation	100°
Max. horizontal radiation	60°
Max. vertical radiation	34°

2.3 Security

The following section covers the cybersecurity legislation aspects that affect the project. Such legislation is covered under the Directive on Security of Network and Information Systems, commonly known as the NIS directive. The NIS directive is the result of a shared effort of the European Committee and member states of the EU, and the first part of the EU-wide cybersecurity legislation. The NIS directive obligates each member country to achieve specified results and leaving them the decision how to do so and which means should be implemented.

2.3.1 CONCERNED ENTITIES

The NIS directive is effective on two main entity categories. The first one is referred to “*operators of essential services*”. This group includes companies from energy, transportation, or financial sectors. Other members of this group are owners of infrastructure where health service entities, banks, water suppliers, etc., run. The second group covers providers of digital services such as Internet browsers, shopping platforms or cloud computing. It is clear that entities from both groups are interested in technologies and solutions developed within iNGENIOUS.



2.3.2 OPERATORS' OBLIGATIONS

Under the NIS directive, operators of essential services have two main responsibilities. The first one is the introduction of the adequate technical and organisational measures to manage the risks posed to the security of network and information systems. The adequacy of measures is strongly bound to the risk assessment and should always depend on the offering services.

The second important task of operators is reporting the security incidents. The NIS directive proposes criteria for establishing thresholds of impact to be reported. Some metrics to consider are:

- The number of users affected by an incident.
- The duration of the incident.
- The geographical spread regarding the area affected by the incident.
- The extent of the disruption of the functioning of the service.
- The extent of the impact on economic and societal activities.

2.3.3 PROVIDERS' OBLIGATIONS

The NIS directive applies to three types of service providers: online marketplaces, online search engines, and cloud computing services. Since providers of such services are often an international corporation, they are selected directly by the EU as concerned by the NIS directive. They must provide the level of security with measures based on the identified risks. Service operators are also encouraged to report incidents to Computer Security Incident Response Team (CSIRT) or the competent authority. The responsibility of reporting the incident depends on the set of information that are accessible to the provider (see Section 2.3.2).

The obligation to notify an incident applies only where the digital service provider has access to the information needed to assess the impact of an incident against those parameters.

2.3.4 RESPONSE TEAMS AND COOPERATION GROUPS

The Computer Security Incident Response Team (CSIRT) is designated by member countries and covers both operators and providers. The NIS directive enumerates requirements and tasks for CSIRTs. In short, CSIRTs are the next line of support for operators and service providers in preventing the incidents and minimising their effects. Countries do not need to establish a CSIRT at national level. It is a good practice instead to create teams that respond to security incidents in designated sectors. Under these circumstances, another important role is the specialised Information Sharing and Analysis Centre (ISAC).

All countries must appoint a single CSIRT on its territory to take the role of single point of contact and to take part in network of national CSIRTs, which is crucial to exchange information on CSIRTs' services, operations and cooperation capabilities and is platform to discussing, exploring, and identifying further forms of operational cooperation.



Another important international body formed under the NIS Directive is the Cooperation Group. It includes the representatives of member countries, the European Committee and the ENISA as the observer.

2.3.5 STRATEGY ON CYBERSECURITY

The NIS directive obligates EU members to establish and introduce a national strategy on network and information systems security, which addresses issues such as:

- Objectives and priorities.
- A governance framework to achieve such objectives and priorities, including roles and responsibilities of government bodies and other relevant actors.
- The identification of measures relating to preparedness, response, and recovery, including cooperation between the public and private sectors.
- An indication of education, awareness-raising, training programmes.
- An indication of research and development plans.
- A risk assessment plan.
- A list of the actors involved in the strategy implementation.

2.4 Privacy and Data Protection

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 functional to the protection of privacy, where the two concepts are not overlapping.

The term '*privacy*' in the legal vocabulary refers to the right to confidentiality of personal information, i.e., the private life of every individual. A natural evolution of the right to privacy is the protection of personal data, and through the technical-legal instrument the legislator protects all the rights connected with personal identity.

The General Data Protection Regulation (GDPR) is the legislation introduced by the European Parliament in [28]. It repeals the *1995 Directive (95/46/EC)* on the protection of individuals about the processing of personal data. The new regulation targets all aspects of European citizens' privacy and data protection, but achieving compliance is an ongoing process. The key difference between the GDPR and the directive is that the GDPR is a regulation, then means that it is a directly enforceable law in all member states, while a directive is a piece of legislation that sets an objective to be achieved by all EU countries and it is up to individual countries.

The GDPR was put into effect on May 25, 2018, after a two-year long adaption period for EU companies and public institutions. It is directly applicable in all Member States and in accordance with the principle of subsidiarity, prevails over the domestic law of Member States in case of conflict with it.



The European Regulation does not define what measures should be taken to avoid threats to data security and violations of data subjects' rights but leaves the data controller maximum freedom about these choices. The main reason why the EU has a new data protection framework is technological change and globalisation since these aspects bring new challenges to personal data protection. The scale of personal data sharing, and collection has increased significantly, and this evolution requires a more robust and consistent data protection framework in the EU.

A complete checklist for handling personal data is provided in Annex A.

2.4.1 APPLICABILITY

There are two possibilities when using the term person, which indicates the protagonist of relationships and activities regulated by law:

- *Natural persons*: All individuals belonging to the human species endowed with legal capacity "*the ability to make manifestations of wills capable of modifying one's legal situation*".
- *Legal person*: Collective organisation constituted by several natural persons, a plurality of natural persons (association, committees, companies) or a patrimony (foundations).

The GDPR is not applicable to companies. According to the European Regulation, the protection of personal data is an exclusive right of the natural person but not of the legal person. However, information on individual companies may constitute personal data if:

- the name of a natural person (such as the owner of a company) is included in the name of the legal person.
- Data collected by a contact form relates to both natural and legal persons (as in the case of company emails).
- In cases of automated processing of personal data, it is difficult to distinguish between data relating to individuals and data relating to legal entities.

In these cases, the rules also apply to all personal data relating to natural persons in the course of a business activity.

The aim of the European legislator is to simplify data management in business-to-business relations. In this sense, in fact, the data of legal persons can be not only collected, but also processed and then communicated to third parties, without the need for a legal basis, and therefore without the legal person being able to claim any rights on its data. The scope of the European Regulation is clearly expressed in Articles 1, 4 and 14 of [28].

2.4.2 ACCOUNTABILITY

The principle of accountability (i.e., empowerment) is one of the pillars of GDPR. The principle is embodied in Article 24 of [28], by virtue of which "*having regard to the nature, scope, context, and purposes of the processing, as well as to the risks of varying degrees of likelihood and severity to the rights and freedoms of natural persons, the controller shall implement appropriate*



technical and organisational measures to ensure, and be able to demonstrate, that the processing is carried out in accordance with this Regulation". Such measures "shall be reviewed and updated as necessary". The term accountability refers precisely to the need for the data controller to introduce mechanisms for internal accountability.

2.4.3 PERSONAL DATA

The definition of personal information or data is extremely broad and includes any information relating to a natural person who is identified or identifiable, even indirectly, by reference to "any information, and which can provide information on his or her characteristics, habits, lifestyle, personal relationships, state of health, economic situation".

Identified refers to a natural person who is known or distinguished in a group whereas identifiable is a person who is not identified yet, but such identification is possible. Particularly important are data allowing direct identification, such as: first name and surname, images, etc.; and data allowing indirect identification, such as: tax code, IP address and cookies (as they identify the browser or the digital device through which the person surfs the net). Other data for identification is the fingerprint or plate number. With the evolution of new technologies, other personal data have taken on a significant role, such as glocalization, providing information on places visited and movements.

2.4.4 SUBJECTS INVOLVED IN DATA TREATMENT

Figure 3 shows the different subjects involved when treating specific data, which are described in this section.

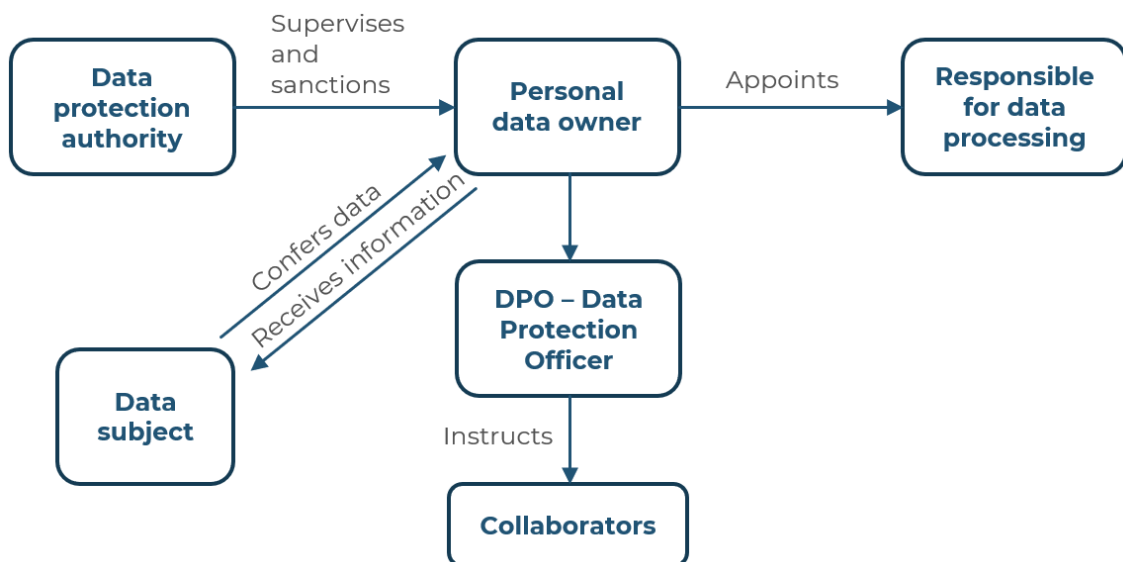


Figure 3. Subjects involved in data treatment.

Data Protection Authority: Supervisory authority who provides the regulatory oversight for GDPR, guidance and advice and, where necessary impose corrective actions or administrative fines.



Personal Data Owner: Natural or legal person, the public authority, service or body which, individually or jointly with others, determines the purposes and instruments of the processing of personal data.

The Personal Data Owner or Responsible of data processing shall appoint a **Data Protection Officer (DPO)**, a person who can guarantee a thorough knowledge of privacy legislation and specific skills in the field, if the processing is carried out by a public authority; or activities require regular and systematic monitoring on a large scale of special categories of data or personal data relating to criminal convictions and offences.

The DPO can instruct **Collaborators** (e.g., employees or trainees). The person to whom the data to process refers is defined as "**Data Subject**" and can only be a natural person and not a company. It has the following rights which must be upheld when processing their personal data. A breach of these rights can result in the maximum fine. The rights are (i) to be informed, (ii) to access, (iii) to rectify, (iv) to erase, (v) to restrict processing, (vi) data portability, (vii) to object.

2.4.5 RISK MANAGEMENT

GDPR requires a risk assessment process to be put in place, in which the risks are identified, and a decision is made on what to do to contain and monitor them. ISO 31000 [29] is the international reference standard for risk management and it allows to identify, prevent, and manage all impending risks through a structured approach. Figure 4 shows the risk management process to follow in the context of this reference.

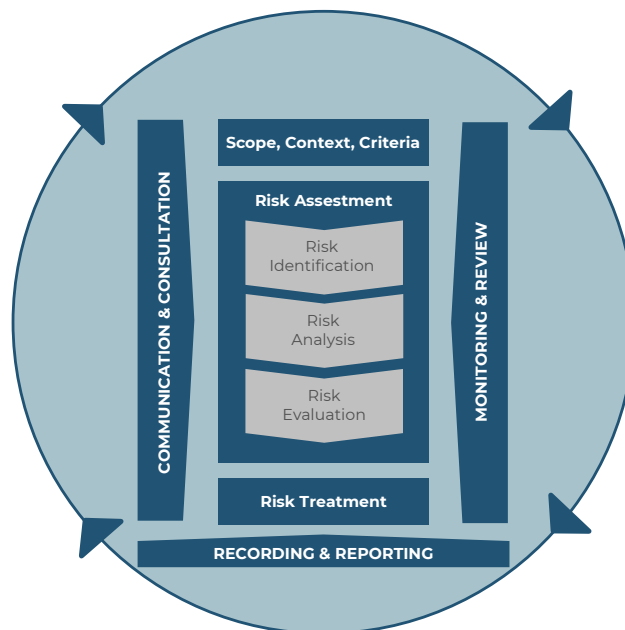


Figure 4. Risk management process.

The risk management process should be an integral part of management and decision-making and integrated into the structure, operations, and processes of the organisation. It can be applied at strategic, operational, programme or project levels. There can be many applications of the risk management process within an organisation, customised to achieve objectives and to suit



the external and internal context in which they are applied. The dynamic and variable nature of human behaviour and culture should be considered throughout the risk management process. Although the risk management process is often presented as sequential, in practice it is iterative.

2.4.6 REGULATION IN THE INTERNATIONAL PANORAMA

The objective of the EU is to uniformly regulate all flows of information that passes through Europe, trying to reorder, through legislation, the digital world dominated by foreign countries. Therefore, even companies that are located outside the EU, but nevertheless process personal data of individuals who are in its territory, in the context of profiling activities, will have to comply with the GDPR rules.

Up to now, users from an EU member state buying online from a website based, in a foreign country were subject to the law of such. However, with the new EU regulation, the data processing rules are no longer applicable. Now it will be up to foreign companies offering their services in the EU to comply with European law.

For instance, in the United States, users are protected above all as consumers and the protection of their privacy is, not by chance, mainly attributed to the Federal Trade Commerce (FTC), which intervenes in this matter protecting personal data as an extension of consumer protection and the legitimacy of fair trade.

Anything that can identify individuals must be controlled. Access to production databases must be monitored, while backups and copies of databases in other environments such as development and testing must have sensitive data masked. Data masking and complementary technologies, such as format-preserving encryption and tokenisation, must be adopted as a key strategy.

2.4.7 APPLICATION TO iNGENIOUS

Recital 14 of the GDPR [28] clarifies that the regulation does not apply to the processing of personal data which concerns legal persons, including their name, form, and contact details. An e-mail address of a legal person would not fall within the scope of the regulation. However, personal data of employees, including their professional e-mail addresses, would fall within the scope of the regulation.

In the context of iNGENIOUS, architecture design and development always have some potential ethical and privacy risks. Protecting personal data from unauthorised or unwarranted access can become critical [30] [31]. The privacy and data protection workflow for iNGENIOUS is shown in Figure 5. The project is supported by a working group including technical/legal experts (DPO contact points) of each partner of the consortium, that can be contacted on request and provide developers with valuable support on data protection and retention. In particular, the project as a whole has a DPO that will contact the necessary experts in order to ensure the privacy and proper management of data in case this is needed in a trial.



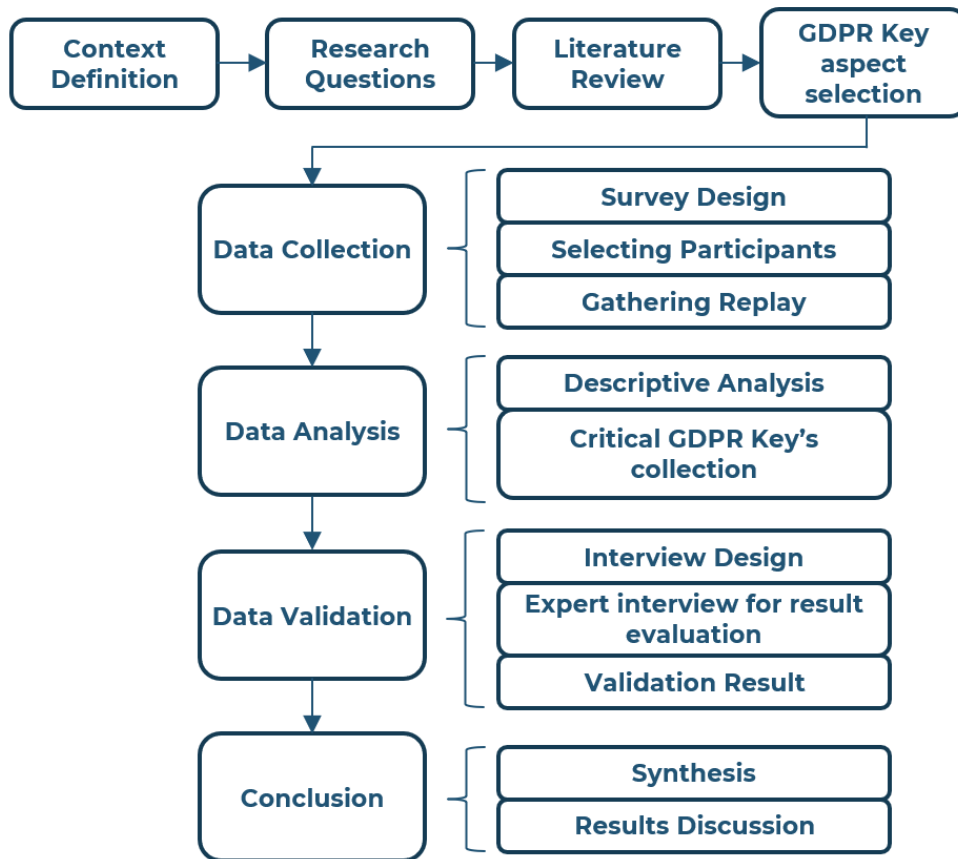


Figure 5. Privacy and data protection workflow for iNGENIOUS.

The committee acts as a contact point for:

- **Context definition:** nature, scope, context, purpose, sources of risk of the case study.
- **Research questions:** processing issues.
- **Literature review:** update to legal literature and cutting-edge theories on information security, data protection, security awareness.
- **GDPR selection of key aspects:** 1) Personal data 2) Data subject 3) Special personal data 4) Data processing.
- **Data collection:** use and purpose of data.
- **Data analysis:** cross-referencing with legislation in the countries involved.
- **Data validation:** compliance with the privacy process considering people, process, and technological aspects.
- **Conclusion:** verdict on people's data and their privacy protection.

2.5 Use of cryptocurrencies

Blockchain technologies allow people and organisations who may not know or trust each other to collectively agree on and permanently record information without a third-party authority [32]. The European blockchain strategy for the use of cryptocurrencies is about the following aspects: building a pan-European public service blockchain, increasing funding for research and innovation, promoting legal certainty, promoting blockchain for



sustainability, supporting blockchain skills development, as well as supporting both interoperability and standards.

EU is engaged in different activities within the blockchain standards community. The organisations involved include: StandICT, ETSI (in particular ISG PDL), CEN and CENELEC via the joint technical committee. EU is also active in multinational and industry led organisations, for example ISO, ISO/IEC JTC1 and ITU-T, as well as open standards organisations such as IEEE, Outcome and Assessment Information Set (OASIS) and the Internet Engineering Task Force (IETF).

Currently, no EU regulation on blockchain has yet been approved. A similar situation concerns efforts in the US, although the work in the US has started earlier. The legislation introduced in the US does not treat cryptocurrencies as foreign currencies, but as property. On the other hand, China has been recently working on introducing its Central Bank Digital Currency (CBDC), and its digital yuan is about to enter beta-testing.

With respect to open Distributed Ledger Technologies (DLTs) such as Bitcoin or Ethereum, the policies have not been defined yet in most countries. Two extreme examples of nation state approaches to cryptocurrencies are: China and El Salvador. China has declared illegal to mine cryptocurrencies, while El Salvador considers that Bitcoin and USD legal tenders must be accepted by every economic entity.

The European Central Bank (ECB) is currently reviewing ramifications of possible introduction of the digital euro. This initiative aims at ensuring that in an increasingly digital environment both citizens and businesses can have access to new forms of money and payment. The ECB intends this digital euro to meet the needs of citizens, while at the same time helping to prevent illicit activities. The digital euro would always act as a complement to cash, not as a substitute for it.

In September 2020, the Commission proposed a pilot regime for institutions wishing to test trading and transaction settlement in crypto-asset form. In the press release of 14 July 2021 [33], the ECB announced the investigation phase. It will last 24 months. The aim is to analyse the needs that a digital euro should meet in order to offer a risk-free, accessible and efficient form of central bank-issued digital money [34], [35], [36]. At this stage, the ECB has not identified any major technical obstacles in relation to the design options analysed and therefore the project is going ahead.

There are some European rules and judgments that mention crypto-assets directly or indirectly:

- Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of use of the financial system for the purposes of money laundering or terrorist financing and amending Directives 2009/138/EC and 2013/36/EU [37].
- Judgment of the Court of Justice of the EU (CJEU, Fifth Chamber). CJEU states that Bitcoin is a virtual currency whose exchange for traditional currencies is exempt from VAT [38].

Other European reports can be found in [39], [40] and [41].



2.6 Regulatory Framework per Use Case

Now that all regulatory aspects have been presented, this section provides a use case-oriented perspective, where regulatory issues affecting the different iNGENIOUS deployment scenarios are discussed. This has been done by providing one table per section, summarising the regulatory environment surrounding each use case.

2.6.1 AUTOMATED ROBOTS WITH HETEROGENEOUS NETWORKS

Table 8. Regulatory Framework of the Automated Robots with Heterogeneous Networks UC.

Regulatory Framework	Activity	Description	Regulation/ Directive	Limitations
Functional Safety	AGVs	Safety requirements and the means for their verification for driverless industrial trucks (and their systems)	ISO 3691-4:2020 Industrial trucks - Safety requirements and verification - Part 4: Driverless industrial trucks and their systems	<p>No requirements for additional hazards:</p> <ul style="list-style-type: none"> • During operation in severe conditions (e.g., extreme climates, freezer applications). • During operation in nuclear environments. • From trucks intended to operate in public zones (in particular ISO 13482). • During operation on a public road. • During operation in explosive environments. • During operation in military applications. • During operation with hygienic requirements. • During operation in ionizing environments. • During transportation of (a) person(s) other than (the) intended rider(s). • When handling loads the nature of which can lead to dangerous situations. • For rider positions with elevation function higher than 1200 mm from the floor/ground to the platform floor.
Functional Safety	Robots	Requirements for the inherently safe design, protective measures, and information for use of robots for an industrial environment.	ISO/DIS 10218-1.2 Robotics — Safety requirements — Part 1: Industrial robots	<p>This ISO document is not applicable to:</p> <ul style="list-style-type: none"> • Underwater. • Law enforcement. • Military (defence). • Airborne and space robots, including outer space. • Medical robots. • Healthcare robots. • Prosthetics and other aids for the physically impaired. • Service robots. • Consumer products, as this is household use to which the public can access. • Lifting or transporting people. • Mobile platforms. • Tele-operated manipulators.
Spectrum	Frequency bands available	Frequency bands will be employed to control AGVs via 5G	<p>Opinion on spectrum related aspects for next-generation wireless systems (5G) - EUROPEAN</p> <p>Spanish Order ETD/666/2020 - LOCAL</p>	Bands available at n77, n78 and n79 frequencies for 5G commercial network.



2.6.2 IMPROVE DRIVERS' SAFETY WITH MR AND HAPTIC SOLUTIONS

Regulatory Framework	Activity	Description	Regulation/ Directive	Limitations
Automated lane-keeping systems	Tele-operated Driving (ToD) operations	Regulation for implementing ALKS	United Nations, "Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System" Economic and Social Council, June 2020.	Regulation and limitations when implementing this type of autonomous systems, such as velocity when the driver is not in control, approval or facing failures.
Spectrum	Frequency bands available	Frequency bands will be employed to control AGVs via 5G mm-wave in the port of Valencia	Opinion on spectrum related aspects for next-generation wireless systems (5G) - EUROPEAN Spanish Order ETD/666/2020 - LOCAL	Bands available at n257, n258, n259, n260, n261 frequencies for 5G.

Note that for the particular use case, we will approach its regulatory framework through the 5GAA cross-working group. Its item called Tele-operated Driving (ToD) aims to describe the requirements and framework needed for remote vehicle operation. The proposed results should reliably enable remote steering and manoeuvring including a human remote driver with both direct and indirect control in an inter-MNO and cross-authority operation.

Currently, there is not any regulation in the world that allows for ToD operations on a day-to-day basis on public roads. There are some examples of legislative work being done to accommodate the latest technological developments, but these are targeting autonomous driving, and not ToD per se.

A good example of this is the regulation on "automated lane-keeping systems" that was adopted by the United Nations in June 2020 [42]. This regulation establishes strict requirements for passenger cars which, once activated, are in primary control of the vehicle. However, the driver can override such systems and can be requested by the system to intervene, at any moment. It stipulates that Automated Lane Keeping Systems (ALKS) can be activated under certain conditions on roads where pedestrians and cyclists are prohibited and which, by design, are equipped with a physical separation that divides the traffic moving in opposite directions.

In its current form, the regulation limits the operational speed of ALKS systems to a maximum of 60 km/h. It also requires that on-board displays used by the driver for activities other than driving when the ALKS is activated shall be automatically suspended as soon as the system issues a transition demand, for instance in advance of the end of an authorised road section. The regulation also lays down requirements on how the driving task shall be safely handed back from the ALKS to the driver, including the capability that the vehicle comes to a stop if the driver does not reply appropriately. The regulation includes the obligation for car manufacturers to introduce driver availability recognition systems. The regulation also introduces an obligation to equip vehicles with a 'black box' called *data storage system for automated driving*, which will record when ALKS is activated.



While awaiting these legislative evolutions, the only way to deploy ToD vehicles will be to integrate them in research and development activities, and not yet in day-to-day operations. For such experiments on public roads, many countries have a legal process of exemptions to test prototype vehicles on public roads under certain conditions. Some examples of such frameworks are the *Dutch Exceptional Transport Exemptions Decree* or more recent *Dutch Experimentation Law on Self-driving Vehicles*. Similarly, Belgium has defined a framework called the *Code of Practice autonomous vehicles*. These are just a few examples of a regulatory framework that can be found in many countries worldwide, allowing for the testing of ToD on public roads, but not for deployment. When focusing on confined areas, and not on public roads, these regulations are not applicable. Therefore, from that perspective, there seem to be no regulatory constraints for deployment of ToD.

2.6.3 TRANSPORTATION PLATFORM HEALTH MONITORING

Table 9. Regulatory Framework of the Transportation Platform Health Monitoring UC.

Regulatory Framework	Activity	Description	Regulation / Directive	Limitations
Functional Safety	Safety of workers	The functional safety of workers in transportation will be measured through HW metrics	IEC61508	The concept design will be restricted by this directive
Fire and Explosion	Fire and Explosion risk in transportation	Fire and explosion risks in transportation will be measured through HW metrics	ATEX IECE	The concept design will be constrained by this regulation

2.6.4 INTER-MODAL ASSET TRACKING VIA IOT AND SATELLITE

Table 10. Regulatory Framework of the Inter-modal Asset Tracking via IoT and Satellite UC.

Regulatory Framework	Activity	Description	Regulation/Directive	Limitations
Spectrum	Frequency bands available	Frequency bands will be employed to provide inter-modal asset tracking services with Satellite, LoRa, Wi-Fi, BT, LTE/LTE-M/NB-IoT connectivity	COMMISSION IMPLEMENTING DECISION (EU) 2019/784 - EUROPEAN Opinion on spectrum related aspects for next-generation wireless systems (5G) - EUROPEAN Spanish Order ETD/666/2020 - LOCAL	Bands available at 700/800 MHz for NB-IoT and LoRa, and 2.1 GHz and 2.6 for LTE commercial network
Data Protection and Privacy	Privacy of sensitive data	Privacy of sensitive data needs to be ensured	General Data Protection Regulation (GDPR) (EU) 2016/679. Only applicable to sensitive data - EUROPEAN	Sensitive data needs to be pseudonymised before sharing and exploiting it during the use case execution
Security	Cybersecurity of all systems and platforms	Ensure cybersecurity of all systems and platforms involved in the use case for delivering data to cloud	EU Cybersecurity Act - EUROPEAN COM (2009) 149 - EUROPEAN ISO/IEC 27000:2012 on Information Technology - INTERNATIONAL NIS Directive. DIRECTIVE (EU) 2016/1148	The cybersecurity of all systems and platforms needs to be ensured before developing a production environment



Security	Carriage of dangerous goods in packaged form	Ensure showcase and security of carriage of dangerous goods	<p>The International Maritime Dangerous Goods Code</p> <p>Agreement concerning the International Carriage of Dangerous Goods by Road</p> <p>Real Decreto 145/1989, National regulation ensuring acceptance, handling, and stowage of dangerous goods.</p> <p>Real Decreto 210/2004 based on Council Directive 93/75/EEC, concerning minimum requirements for vessels entering or leaving Community ports and carrying dangerous or polluting goods.</p>	The security of stowage, handling and carriage of dangerous goods needs to be ensured both at maritime and inland leg
----------	----------------------------------------------	-------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------

2.6.5 SITUATIONAL UNDERSTANDING AND PREDICTIVE MODELS IN SMART LOGISTICS SCENARIOS

Table 11. Regulatory Framework of the Situational Understanding and Predictive Models in Smart Logistics Scenarios UC.

Regulatory Framework	Activity	Description	Regulation/Directive	Limitations
Spectrum	Frequency bands available	Frequency bands will be employed to provide container tracking services with LTE/LTE-M/NB-IoT connectivity	<p>COMMISSION IMPLEMENTING DECISION (EU) 2019/784 - EUROPEAN</p> <p>Opinion on spectrum related aspects for next-generation wireless systems (5G) - EUROPEAN</p> <p>Spanish Order ETD/666/2020 - LOCAL</p>	Bands available at 700 MHz (NB-IoT), 2.1 GHz and 2.6 GHz for LTE commercial network
Data Protection and Privacy	Privacy of sensitive data	Privacy of sensitive data such as truck plate numbers needs to be ensured	General Data Protection Regulation (GDPR) (EU) 2016/679. Only applicable to sensitive data - EUROPEAN	Sensitive data needs to be pseudonymised before sharing and exploiting it during the use case execution
Security	Cybersecurity of port systems and platforms	Ensure cybersecurity of all systems and platforms involved in the use case for ingesting data at maritime ports	<p>EU Cybersecurity Act - EUROPEAN</p> <p>COM (2009) 149 - EUROPEAN</p> <p>ISO/IEC 27000:2012 on Information Technology - INTERNATIONAL</p> <p>NIS Directive. DIRECTIVE (EU) 2016/1148</p>	The cybersecurity of all systems and platforms needs to be ensured before developing a production environment

2.6.6 SUPPLY CHAIN ECOSYSTEM INTEGRATION

Table 12. Regulatory Framework of the Supply Chain Ecosystem Integration UC.

Regulatory Framework	Activity	Description	Regulation/Directive	Limitations
Data Protection and Privacy	Privacy of sensitive data	Privacy of sensitive data needs to be ensured	General Data Protection Regulation (GDPR) (EU) 2016/679. Only applicable to sensitive data - EUROPEAN	Sensitive data needs to be pseudonymised before sharing and exploiting it during the use case execution.



3 Business Models

The following sections present and discuss the second block of D2.3, i.e., iNGENIOUS business models. The section has been divided into three main parts. The first part includes a PESTEL analysis, which provides the macroenvironmental factors that are not precisely related to the project itself. This is necessary to understand the current business framework and provide some context. Next, the different technology solutions that may bring new business models and opportunities to the consortium are presented. Finally, the deliverable discusses the potential business models that could be derived from each one of the use case implementations. Note that this part of the deliverable is expected to be expanded upon in D2.5, which will go deeper on this area as well as analyse and discuss innovative and outbreking business models for the future of IoT technologies.

3.1 PESTEL Analysis

A company is influenced by various factors. Some are related with the firm itself, such as the organisational structure, values, or relationships with customers and suppliers. Others depend on the industry, like specific regulations or competitors. There is a third level corresponding to the most external layer. This includes environmental factors unrelated to the company or the industry but that can directly affect their performance.

The PESTEL framework will be employed to analyse the macro-environmental factors corresponding to the external layer, by dividing them into six fields: political, economic, social, technological, environmental, and legal. For example, one social aspect that can influence a 5G related company's business model is the adaption rate of new technologies among the population. If the citizens of a country are inertial in terms of technologically change it will directly affect the sales, lowering the rate compared to a country without this issue. Another example could be a recession in the economy. This is an economical aspect that affects the company.

A single PESTEL analysis covers the whole project macroenvironment. Different aspects about the EU will be gathered in these six categories.

3.1.1 POLITICAL

The EU includes 27 countries physically allocated in Europe. It was created in 1951, when six European countries started to cooperate economically. These countries were Belgium, Germany, France, Italy, Luxembourg, and the Netherlands. Later, more countries joined the EU [43]. Just one country left the EU since its beginning, i.e., the United Kingdom effectively in January 2020.

One of the factors that affect the project, is the fact that the EU provides political stability and a solid union within the European territory. The EU takes care of all member states and provides support when needed in case of crisis, with, for example, a recovery plan in the case of pandemic [44]. The EU also foments alignment among members when taking decisions, acting as a unique country in some political decisions such as the COVID-19 vaccination strategy [45], where common areas enabled the optimisation of the



vaccination process in the continent. The alignment in this decision making also contributes to the political stability.

All member states in the EU are formal democracies, divided in 6 constitutional monarchies and 21 republics. This guarantees a level of freedom and justice that some countries cannot provide.

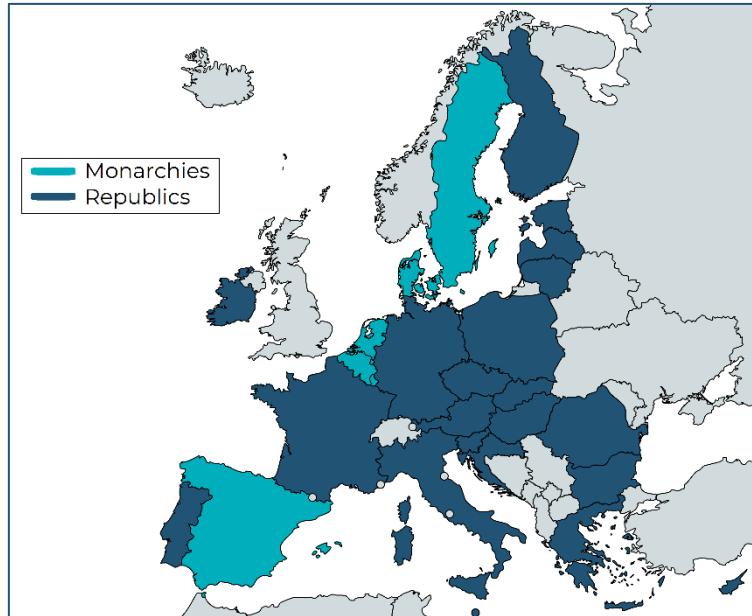


Figure 6. EU member states divided into monarchies and republics.

With globalisation, relationships among countries are key factors that can enable new opportunities and permit the establishment of commercial relationships between companies of those countries. In addition, the EU has fluid relationships with one of the largest economic powers in the world: the United States of America (US) [46] [47].

There is a part of the European population that does not believe in the EU as a useful entity, neither does not see the utility of it. This way of thinking is called “Euroscepticism” [48], and in the last years has been boosted by the Brexit, i.e., the exit of the United Kingdom from the EU. In June 2016, there was a referendum to make the population participant of the decision of exiting or not the EU. The results ended up in an affirmative answer. Later, in January 2020, the UK initiated the transition period outside the EU, and such decision has fomented the Euroscepticism in the rest of Europe.

Another negative factor affecting politics is the migratory crisis. The EU has a migratory policy [49], but recently in 2021, there has been a significant increase of people, especially from Africa, entering into the south of Europe. This crisis has created arguments among EU countries about refugees and how to solve the crisis.

Table 13 summarises the different factors that were discussed above and provides a positive/negative impact value that goes from 1 to 3 (being 1 low impact and 3 high impact). The colour code is the following: red – negative, grey – neutral, green – positive.



Table 13. Political factors around the iNGENIOUS project.

Impact	Factor	Description
● ●	Relationship with USA and other countries	Good political relationships with the US and other countries.
●	Political Stability and solid union in Europe	The stability in the political structures in Europe is high. The implication of the EU contributes in this.
● ● ●	Democracies	All member states in the European Union are democracies.
●	Euroscepticism due to Brexit	Doubts about the utility of the European Union triggered by the Brexit.
●	Migratory crisis	Arguments among countries in Europe due to disagreements.
● ●	Alignment taking decisions	EU common responses such as vaccination strategy in COVID crisis or international opinions.

3.1.2 ECONOMIC

In the economic part, Europe is one of the most developed areas in the world, and its economic macro-trend is growing [50]. However, the COVID-19 crisis has produced an economic recession with a high impact, all around the globe and in particular in the EU [51].

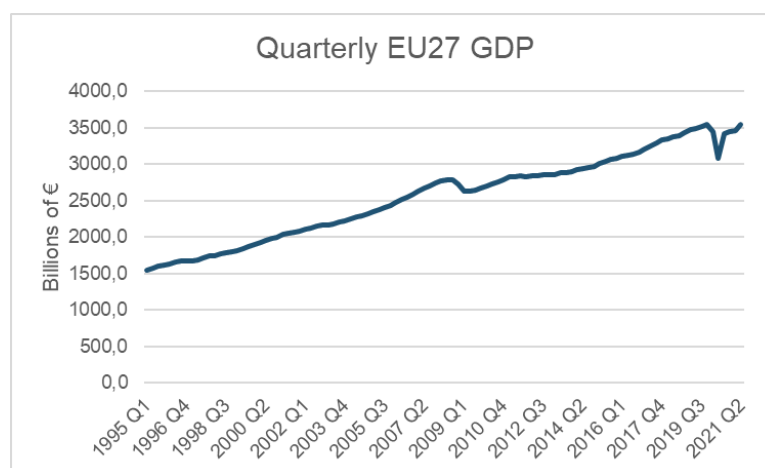


Figure 7. Gross Domestic Product (GDP) evolution in billions of Euros [52].

Figure 7 shows the aggregated Gross Domestic Product (GDP) of all EU countries, represented quarterly (i.e., four measures per year are done). There is a growing global trend, and it is easy to detect the two main economic crisis that took place in Europe, the one in 2007-2009, and the COVID-19 crisis in 2020. Note that this chart does not include the UK as an EU member state⁴.

⁴ Data from 2020 does not include UK, so in essence it will look like a drastic drop. UK has been removed for a fair comparison among all years.



The EU has a common currency: the Euro (EUR, €). It is the official currency in 19 of the 27 countries of the EU [53]. Seven out of the eight members that do not use the Euro in their economy are working on adopting it in the coming years, since this was a condition to enter the EU. Therefore, Denmark is the only country who is not committed to switch to the Euro. The current currencies as of November 2021 in the EU members are shown in Table 14.





Table 14. Current currencies used in EU member states.

Currency	Countries
Euro (EUR)	Austria, Belgium, Cyprus, Estonia, Finland, France, Germany, Greece, Ireland, Italy, Latvia, Lithuania, Luxemburg, Malta, Netherlands, Portugal, Slovakia, Slovenia, Spain
Bulgarian lev (BGN)	Bulgaria
Croatian Kuna (HRK)	Croatia
Czech koruna (CZK)	Czech Republic
Danish krone (DKK)	Denmark
Hungarian Forint (HUF)	Hungary
Polish Złoty (PLN)	Poland
Romanian Leu (RON)	Romania
Swedish krona (SEK)	Sweden

The Euro is consolidated as one of the most robust currencies in the world and with more international influence [54]. The Euro has a higher value than the US Dollar (USD), with an exchange rate of 1 EUR = 1.12 USD (*consulted on 24/11/2021*) [55].

Another important aspect to highlight in the context of iNGENIOUS is the funding of European R&D projects. The EU actively promotes R&D projects with programmes such as Horizon 2020 [56] and Horizon Europe [57] to develop and validate technological innovations.

Table 15. Economic factors around the iNGENIOUS project.

Impact	Factor	Description
	Economic recession due to COVID	COVID-19, with all its implications, has produced a recession in economic terms. Its impact has been huge all around the globe.
	Euro currency stability and worldwide influence	Common currency in 19 of the 27 EU countries. The euro is a stable currency and with international influence.
	Foreign exchange	The euro has high value (1 Eur = 1.16 USD, <i>checked the 20/10/2021</i>).
	EU support and funding for R&D projects	The EU promotes R&D projects with programmes like H2020 and Horizon



		Europe, providing budgets to develop the proposed technological innovations.
●	Growth macro-trend	Although in short terms there might be a crisis (COVID-19), the macro-trend is growing.
●	EU is an economic power	EU is one of the world economic powers.

3.1.3 SOCIAL

Social behaviour has changed in the last decades, mainly due to technological advances and globalisation. In the EU, we are living in a society that uses technology on a daily basis. Therefore, technology is playing a key role in every aspect of our lives. There is a clear rapidness of the market to adopt a new technology for solving a problem or improving a service [58] [59] [60]. Years ago, it would have taken much more time to society to adapt to a certain new technology. This factor may boost even more the technological advances, making its trend exponential.



Another aspect to analyse is the population. The EU covers over 4 million km² and has 447.7 million inhabitants (*consulted on 21/10/2021*) [61]. The birth rate is less than the death rate in the EU, according to 2020 and 2021 estimations [62]. This means that the population growth rate in the European Union is negative.

A modern society is also driven by mobility and travelling. Nowadays, the access to travel is higher than years ago thanks to the globalisation, flight access in terms of price and quantity [63], and, in Europe, thanks to the free movement within the Schengen area [64]. However, despite this increasing trend, the COVID-19 crisis caused a drop in travel, due to restrictions. Note that this impact has been different in the US [65] and the EU [66].

Table 16. Social factors around the iNGENIOUS project.

Impact	Factor	Description
● ●	Market rapid adoption of new technologies	Rapidness of the market to adopt new technologies.
●	Population in EU	447.7 million, with a birth rate of 9.5 and death rate: 10.7
●	Diversity social acceptance	Diversity is widely accepted in the EU.
● ●	Mobility and travel reduction due to COVID	COVID-19 has reduced mobility due to fear and governmental restrictions.
●	Social behaviour changes due to COVID	COVID-19 has changed the way people behave socially, generally reducing social life.



	Technological society	The society is based on technology, and technology is becoming more important each day.
	Easiness and accessibility to travel	Thanks to i) free movement in shengen area, and ii) flight access (price and quantity).







3.1.4 TECHNOLOGICAL

The COVID-19 crisis has boosted both digitalisation and technological advances. There is an increase in the number of connected devices and digitised tasks. Teleworking has been a trend in the last years [67]. The lockdown and restrictions also obligated us to adapt to conference calls and working remotely.

In terms of R&D projects, the EU promotes programmes such as Horizon 2020 or Horizon Europe, fomenting the technological innovation. This was already mentioned in the economic aspects, but it is also directly translated in new technologies. Among this European projects, there is a huge number of 5G and IoT projects. For instance, in the 5G Infrastructure Public Private Partnership (5GPPP) website [68], there are more than 70 projects related to 5G. Moreover, within the Next Generation IoT (NG-IoT) framework [69], there is a wide number of projects related to IoT, including iNGENIOUS.

Among the industry, the connection of all type of devices to the internet in order to control, manage and gather data from the processes is becoming a global trend. The industry 4.0 revolution is transforming the industry, becoming more intelligent and optimised.

Table 17. Technological factors around the iNGENIOUS project.

Impact	Factor	Description
	Technology innovations	Companies and public entities stimulate technological innovation.
	Increment of teleworking	Teleworking is more present than before thanks to technological advances. COVID-19 has also fomented teleworking.
	Digitisation	We live in the digital era, with an increase in the number of connected devices and digitised tasks.
	EU leadership in technological progress	The EU has a privileged position in technological progress.
	Global trend to connect objects (IoT)	There is a trend of connecting all type of devices.
	R&D activities and innovation, EU promotion of R&D projects	R&D activities are promoted by the EU with programmes such as H2020 or Horizon Europe.



3.1.5 ENVIRONMENTAL

There is high concern about climate change in the EU [70], which is promoting green technologies, fighting it, and reducing pollution. This opens up new opportunities and funding for projects that use green technologies. The EU released the so-called “European Green Deal” [71], investing one third of the 1.8 trillion Euro from the NextGenerationEU recovery plan. At the same time, this concern about the environment has created hard regulations that limit some aspects as the CO2 emissions, plastic use, or Electromagnetic Field (EMF) levels. These limits may reduce the efficiency of some processes and companies as they cannot do certain activities.

Table 18. Environmental factors around the iNGENIOUS project.

Impact	Factor	Description
●	Funds for green technologies	Green technologies to reduce the climate change impact are opening up opportunities and funding.
● ●	Limits and regulations	Limits on CO ₂ emissions, plastic use, and EMF levels.
●	Recycling	Higher concern of recycling

3.1.6 LEGAL

One legal aspect to bear in mind is data protection. Across the EU, data protection is entrusted to GDPR. As explained in Section 2.4, it is the strictest privacy and security law in the world. It ensures that users' data rights are properly protected. This regulation requires companies to handle data with care and, those who violate its privacy and security standards, impose fines with penalties.

Access to licensed spectrum also needs to be regulated. In case of Spain the CNAF [20] is the regulatory organism, and the PNRF in case of Italy. Operators get access to mobile frequency bands through auction. Spectrum is limited, so getting access to it is an important aspect (see Section 2.1).

Intellectual properties are another topic to consider. They are protected thanks to legal mechanisms. The EC defines the Intellectual property rights in [72]. These legal mechanisms are used to protect the companies or entities creations from the competency for a limited time of period.

Table 19. Legal factors around the iNGENIOUS project.

Impact	Factor	Description
●	GDPR strict regulations	Data protection is a huge concern nowadays, and it is strictly regulated.
● ●	Spectrum access difficulties	Spectrum is a scarce resource and getting access to it for most of the activities includes obtaining a license.
●	Intellectual Property protection mechanisms	Intellectual Property can be protected thanks to legal mechanisms



3.1.7 SUMMARY

Figure 8 provides an overview of the different impacts considered and discussed throughout this PESTEL analysis. The representation shows both negative (left) and positive (right) impacts. The length represents the considered impact in the context of iNGENIOUS.

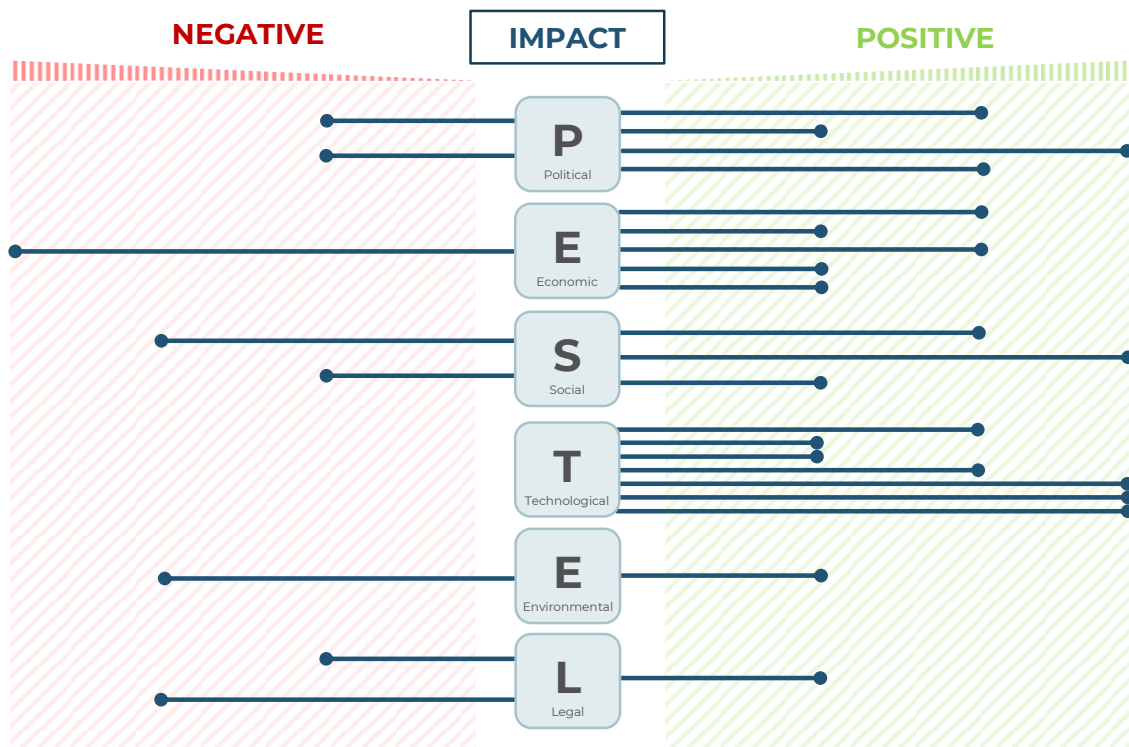


Figure 8. PESTEL impact for iNGENIOUS.

It can be observed that in the political, economic, and technological terms, the macro-frame can be considered positive overall. This means that there are good conditions in these areas where the project is carried out that may facilitate and boost our activities. In the legal area, the impact is more negative than positive. This is usually an area that slows down some procedures and therefore the development of the project. Both environmental and social areas can be considered as neutral.

3.2 Technology Enablers

3.2.1 NON-PUBLIC NETWORKS

NPN is the term adopted by the 3GPP organisation to identify a network that provides mobile services for a dedicated and clearly defined set of users or 'things' that are usually part of a single organisation. NPNs can provide the support needed to implement the "extreme mobile broadband" requirements requested by the manufacturing sector to enable the Industrial Internet of Thing (IIoT) service implementation.

In contrast to a network that offers mobile network services to the public audience, a 5G NPN provides 5G network services to a clearly defined user organisation or group of organisations. It is deployed in a variety of configuration on the organisation's defined premises, such as a campus or a factory, utilizing both virtual and physical elements.

An NPN may be deployed as a:

- **Standalone Non-Public Network (SNPN):** operated by an NPN operator and not relying on network functions provided by a PLMN. The network is deployed as an independent, standalone network and all network functions are located inside the logical perimeter of the defined premises (e.g., factory) and the NPN is separate from the public network.
- **Public Network Integrated NPN (PNI-NPN):** a non-public network deployed with the support of a PLMN, using network slices or Closed Access Group (CAG) cells or a combination of both. The CAG identifies a group of subscribers who have access to one or more cells associated to the CAG and prevents the UEs non authorised to access the NPN. In this case the deployment can be a combination of public and non-public networks, assuming that certain use cases on the defined premises can be supported entirely by the public network, whereas others require a dedicated NPN. The NPN and the public network can share part of the radio access network, while other network functions remain segregated. All data flows related to the NPN traffic portion are within the logical perimeter of the defined premises (e.g., factory), and the public network traffic portion is transferred to the public network.

Non-public networks can be desirable for several reasons:

- High quality-of-service requirements.
- High security requirements, met by dedicated security credentials.
- Isolation from other networks, as a form of protection against malfunctions in the public mobile network. Also, isolation may be desirable for reasons of performance, security, privacy, and safety.
- A non-public network makes it easier to identify responsibility for availability, maintenance, and operation.

NPNs are flexible and tailorable solutions provided by telco operators that allow Communication Service Providers (CSPs) to decide their network focus and how to differentiate their offering to enterprise customers.

Nowadays, there is a rapidly growing momentum for this type of networks. In fact, there is an increasing demand from industries and enterprises for dedicated private cellular networks and a high priority for CSPs to address the opportunity of IIoT adoption. To stay competitive, factories and warehouses must leverage the IIoT and digitalisation to become much more agile and efficient, moving from wired to wireless cellular connectivity, that is able to bring the requested level of flexibility.



3.2.1.1 5G-IoT as a key enabler

5G is a key enabler for implementing NPN networks able to support IIoT and Industry 4.0 applications. 5G is the first wireless technology designed specifically to meet industrial requirements with ultra-low latency, high network availability, and high device density capabilities, guaranteeing on the other end connectivity of large numbers of devices and allowing large quantities of data to be aggregated and delivered from shop floors to remote data centers and cloud-based systems.

According to Business Wire [73], the US private LTE and 5G network market size is anticipated to reach USD 5.68 billion by 2027, expanding at a Compound Annual Growth Rate (CAGR) of 17.0% from 2020 to 2027. The rising adoption of a NPN for IoT applications, industrial use cases, and the Industry 4.0 revolution are some of the critical factors responsible for that market growth. Similarly, according to Mobile Experts [74], the global private LTE and 5G equipment and services market to grow at around 20% CAGR to about \$10 billion in 2025.

3.2.1.2 Flexible RAN deployments for NPNs

In contrast to a standard Radio Access Network (RAN) such as 5G-NR, which is designed for a wide range of use cases and random environment, flexible RAN allows private network operators to customise the air Interface based on deterministic prerequisites. In particular, to optimise the physical (PHY) and medium access control (MAC) layers, a design based on the application requirements, number of connected nodes, and the wireless channel in the covered vicinity is needed.

The interconnection with the transport layer is achieved by means of logical channels defined according to standards. One concrete application is for industrial networks. In this case, the flexible RAN is used to replace the wired bus, and the transport layer is the industrial ethernet. The PHY parameters are set according to link data rate, reliability, and latency, in addition to device mobility, whereas the MAC is designed for deterministic access.

The realisation of flexible RAN involves using a tuneable software-defined radio (SDR) frontend, and a reprogrammable signal processing platform. With that, the flexible RAN allows the integration of beyond-the-standard PHY/MAC solutions in channel coding, modulation and waveform, and MAC design, which opens the door to small innovations to be exploited in businesses.

3.2.2 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. It enables telco operators and service providers to maximise the use and revenue coming from precious resources, dedicating them for critical services, while still offering regular non-premium services with lower quality guaranteed. In other words, network slicing allows to mix the benefits of 5G public and private networks, thus combining coverage and convenience of public 5G subscriptions with traffic isolation, high customisation, and security of private networks.



In practice, 5G network slicing can bring new customers to telco operators and service providers, e.g., among those vertical sectors interested in the capabilities of 5G, like for example industry 4.0 and port logistics, that can leverage on the delivery of private 5G networks. Therefore, this allows telco operators and service providers to expand their offer and targeted markets, thus capturing larger parts of the value chain.

In this context, network slicing can enable a different business model with higher pricing. High performance demanding vertical use cases require highly customised and tailored services, that can be offered at higher costs with respect to traditional “best-effort” services offered through public 5G networks.

Said that, network slicing enables new business models and value chains, as it opens opportunities for telecom operators and service providers to work more and more closely with a wide range of vertical industries covering multiple parts of the value chain, from provider of infrastructures and logical networks, managed services, and integrated co-branded solutions. Indeed, the delivery of multiple logical networks on top of their shared infrastructures allows to onboard new customers by providing customised and isolated end-to-end virtual networks. Therefore, network slicing brings new business relationships and possibly go-to-market roles for telecom operators and service providers, that can leverage on higher flexibility and potential for customisation of their offers, such as:

- **Business to customer (B2C):** In this scenario, the slice consumer is the final end user of the service offered, to whom the telecom operator or service provider charges a premium service for high guaranteed and customised performances.
- **Business to business (B2B):** In this scenario the slice consumer is another business actor (e.g., a vertical industry, another service provider, a government entity) that uses the slice to implement and support an internal use case or service.
- **Business to business to business (B2B2B):** The slice consumer itself uses the slice delivered by the telecom operator or service to further sell and offer services on top it to its customers to deliver customised use cases. In this case the business chain could be even longer with the second customer selling in turn slice-enabled services to another business entity.

Following this direction, from a standardisation point of view, 3GPP has also defined business role models for network slicing as part of 3GPP TR 22.830 [75]. In particular, in the context of 3GPP, 5G and network slicing open the door to new trusted relationships between Mobile Network Operators and 3rd parties, allowing 3rd parties more control of system capabilities. In particular, three main role models are defined:

- The MNO owns and manages both the access and core network.
- An MNO owns and manages the core network, and the access network is shared among multiple operators (i.e., RAN sharing).
- Only part of the network is owned and/or managed by the MNO, with other parts being owned and/or managed by a 3rd party.



While the first two models are applicable to previous generation 3GPP systems (e.g., 3G and 4G), with 5G and network slicing it is expected that 3rd parties can take on the role of an MNO, thus operating their own network. Here, for example, a third party can be a vertical industry. On the other hand, for the third model above, network slicing opens up different options depending on the type of trusted relationships between MNOs and 3rd parties. In particular, in this case, [75] defines four potential business relationship models:

- MNO provides the virtual/physical infrastructure and Virtual Network Functions (VNFs), while a 3rd party uses the functionality provided by the MNO.
- MNO provides the virtual/physical infrastructure and (V)NFs; a 3rd party manages some VNFs via dedicated APIs exposed by the MNO.
- MNO provides virtual/physical infrastructure; a 3rd party provides some of the VNFs.
- a 3rd party provides and manages some of the virtual/physical infrastructure and VNFs.

Moreover, the 5G core needs to include additional network functions that allow the operator of the private network to define network slices that can be allocated to different devices individually or as a group. This new Network Slice Management (NSM) application function (AF) can be instantiated internally as part of the core functions or can be accessible from external applications through Network Exposure Function (NEF). As shown in next figure the NSM-AF design requires a graphical user Interface (GUI) if the network slicing is managed directly by the operator as part of own network management system. The NSM-AF requires 3GPP standard endpoint of the NSM functionality is requested through NEF. Its implementation in the 5G core is shown in Figure 9.

Including network slicing as part of private 5G network enables new business models where the operator can slice the network for own usage to separate and allocate different network resources to different devices. Moreover, the slices in the private 5G network could be commercialised and offered to other operators or service providers that require extra capacity or additional coverage. Therefore, the network slices could be leased or rented to external users for certain period of time.

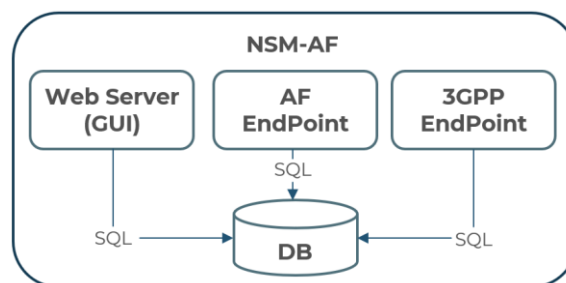


Figure 9. NSM-AF functionality implementation at the 5G core.



3.2.3 TACTILE APPLICATIONS APIS

Tactile applications are characterised by a real-time end-to-end (E2E) response, which implies low-latency and high reliability. The concrete E2E requirements are determined based on the application and the involved devices. Fulfilling these requirements demands cross layer development, from encoding of the application layer data to the transmission of link layer packets.

Considering the network as a distributed computation platform with a variety of connected devices, storage, and processing resources, it is necessary to design a real-time operating system that abstracts the hardware and exposes application programming Interfaces (APIs) to application developers. The operating system is also responsible for the configuration of communications links, synchronisation, and scheduling. Different APIs are to be developed for data acquisition and encoding, which are equivalent to device drivers. Moreover, while the tactile applications consist of control loops, control algorithms are part of low-level libraries. On top of that, end-user APIs provide high level of abstraction for application development with seamless experience.

This model will bring the concepts of computer and software engineering to the tactile network. A specific exploitation is in a private industrial network. The tactile APIs will enable fast development of applications to reuse the available devices such as robot arms and AGVs for performing customised tasks.

3.2.4 CRYPTOCURRENCIES

The project is focusing on a narrowed definition of cryptocurrencies, that includes only open and decentralised ones. In this sense, cryptocurrencies are a new phenomenon that is not only technological, but also political, economic, and social, with potential impact on the environment. Using cryptocurrencies in the project gives legitimacy for them and can initialise some deeper discussion about their usefulness in the developing world.

Cryptocurrencies implement several consensus algorithms that reflect users' needs and beliefs of their creators. The project has put focus on some specific technological features of cryptocurrencies, ledger immutability in particular, rather than their economic aspects.

Cryptocurrencies are the native tokens associated to DLTs. The iNGENIOUS project will utilise multiple DLTs, i.e., Bitcoin, Ethereum, Hyperledger (with TradeLens) and IOTA. Three of them, Bitcoin, Ethereum and IOTA, have native tokens associated with them, that is, the cryptocurrencies BTC, ETH, and IOTA respectively.

Note that each DLT implements different consensus algorithm. This consensus can be viewed as an agreement between the users on some set of rules and how to agree on the *true* state of the system. In summary:

- **Bitcoin** is focused on personal freedom and ability to have full control over one's possession with sound money aspirations.



- **Ethereum** is a platform for smart contracts and decentralised applications, Web3.0 in short.
- **IOTA** focuses on low energy devices and quick transactions in IoT world.

Bitcoin consensus algorithm is based on Proof-of-Work. IOTA uses so called Tangle with a central server called Coordinator (with plans to remove it at some point). Ethereum uses Proof-of-Work (PoW), but since 2015 efforts are made to migrate it to Proof-of-Stake [76].

3.2.4.1 Political impact

From a political perspective, the most impactful cryptocurrency is Bitcoin. It can potentially serve the same utility as gold, but with much easier audit, proof of reserves and faster settlements. It can also allow nation states to avoid sanctions [77]. On the other hand, there is Ethereum and other cryptocurrencies, which allow for closer cooperation between developers and officials [78], and therefore are a better fit for fighting crime and money laundering, since they are not that focused on decentralisation and censorship resistance, but on the usability.

3.2.4.2 Social impact

There are up to 1.7 billion adults unbanked in the world [79]. Bitcoin and other cryptocurrencies provide services in a similar way than banks, but easier in terms of know-your-customer requirements. This allows previously unbanked people to transact and store value without need of banks. Cryptocurrencies can also be used to empower women and create more inclusive societies. For example, Bitcoin can be used to pay women for work in the countries, where woman can't have her own bank account [80].

Cryptocurrencies may allow for saving in the countries hit by hyperinflation [81]. It allows for freedom of speech, for example Wikileaks was denied bank services, but it survived thanks to Bitcoin payments, the same is for Gab and other oppressed or excluded from the public debate [82] [83] [84].

Bitcoin and other cryptocurrencies also allow for remittances that are cheaper and safer. For example, smart contract capabilities and immutability of DLTs bound with cryptocurrencies can reduce cost for verification of data and contractual arrangements.

3.2.4.3 Environmental impact

The most controversial topic is the environmental impact of a wide cryptocurrency usage. The most time proven and currently widely used consensus method is proof-of-work. It is present in two most widely used cryptocurrencies, i.e., Bitcoin and Ethereum.

The immutability and security of DLT is protected by the energy used to perform PoW. This security model has a feature that for the attacker to modify older blocks, it would have to use approximately the same energy as the one that protected it. It proves to be practically impossible. Even in the case of smaller PoW cryptocurrencies, were the energy expenditure to attack them is many orders of magnitude lower, double spending attacks were performed



only for the limited amount of time and didn't destroy the cryptocurrency. And if the PoW is high enough, like for instance Bitcoin and Ethereum, double-spend attacks were never successful.

The growing energy usage brings concerns that it is very inefficient way of protecting the ledger. The critics say that growing energy consumption of Bitcoin is harmful for the environment [85].

However, there are claims, and projects that show that in longer turn, it could be, counterintuitively, be beneficial for the Earth [86]. There are direct effects, such as allowing renewable energy power plants to be profitable and provide energy to grid in times of crisis [87].

There are also speculations, that overall energy consumption in the society with “sound money” will consume less resources, because it will be more profitable to save, than spend immediately.

3.3 Business Models per Use Case

As stated along the document, the iNGENIOUS project consists of six innovative use cases where new technologies related to 5G and IoT are being applied to improve the performance of supply chain activities. The technologies used in these scenarios make it possible to enable new market niches and sustainable business models. In this section, business models will be developed through a Business Model Canvas for each specific use case. It is a widely-used template that will allow us to see the whole business model around a use case in just one place. It divides the strategy in nine different boxes: value proposition, customer relationship, customer segments, channels, key partners, key activities, key resources, cost structure and revenue streams.

The Business Model Canvas tables per use case are provided in the following pages.



3.3.1 AUTOMATED ROBOTS WITH HETEROGENEOUS NETWORKS

Table 20. Business Model Canvas of the Automated Robots with Heterogeneous Networks UC.

Key partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
<p>Industrial factory is the end user of the robotic application and is needed to provide authorisation for the installation of equipment.</p> <p>5G Antenna deployment company to install the 5G millimetre wave antenna to provide coverage to the AGV and the robot.</p> <p>Robot integrator company to configure and supervise the performance of the robotic application.</p> <p>Robot manufacturer company to perform adaptation in AGVs and robots to allow the 5G-based control.</p> <p>Data protection and privacy entities to ensure the security and privacy of data.</p>	<p>Installation of 5G antenna equipment.</p> <p>Procurement of AGV, robotic arm and 3D camera.</p> <p>Development of the robotic application.</p> <p>Ensuring that the 5G coverage complies with the KPI.</p> <p>End-to-End robotic application communications data path.</p> <p>Data recompilation from tele-operation and coverage in order to accomplish the QoS.</p>	<p>Improve the efficiency of the computational resources. Multiple robots share the edge computational resources.</p> <p>Reduce the cost of hardware, electronics, and energy to automate the systems.</p> <p>Improve the redundancy of the systems</p> <p>Reduce the necessity of professional robot operator in every industrial area, enabling the capacity of controlling several robots at different localisations.</p>	<p>Industrial factories will ease the access to 5G equipment in order to define the necessities at the factory.</p> <p>Robot integrator company and robot manufacturer company will work together to enhance the capabilities of the 5G-controlled robotic applications</p>	<p>Industrial factories</p> <p>Robotic integrators</p>
	<p>Key Resources</p> <p>5G coverage.</p> <p>AGV enabled with 5G comm</p> <p>Robotic arm enabled with 5G comm</p> <p>3D camera</p> <p>Computational and storage resources.</p>		<p>Channels</p> <p>Trade fairs</p> <p>Social media</p> <p>Journals</p>	
<p>Cost Structure</p> <p>Procurement and installation of the 5G antenna equipment</p> <p>Procurement and configuration of the AGV</p> <p>Procurement and configuration of the Robot</p>		<p>Revenue Streams</p> <p>Sale/renting of robots</p> <p>Sale/renting of AGVs</p> <p>5G-controlled robotic application as a service</p>		

3.3.2 IMPROVE DRIVERS' SAFETY WITH MR AND HAPTIC SOLUTIONS

Table 21. Business Model Canvas for the Improve Drivers' Safety with MR and Haptic Solutions UC.

Key partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
<p>Port authorities and port terminals are needed to give access to the port infrastructure and authorisation for the installation of equipment.</p> <p>5G antenna deployment company is needed to install the 5G millimetre wave antenna to provide coverage to AGVs.</p>	<p>Installation of 5G antenna equipment.</p> <p>Procurement of ASTI's AGV.</p> <p>Procurement and installation of the immersive cockpit.</p> <p>Development of the immersive cockpit application (interface, data visualisation, haptic data transmission, etc).</p>	<p>Allow a safe driving performance in which potential hazardous situations given on industrial environment can be avoided</p> <p>Improve situational understanding and identify the potential automatization of industrial operations.</p> <p>Reduce the necessity of</p>	<p>Port authorities and terminals will ease the access to the tele-operation decisions in order to define the necessities at the Port.</p> <p>Tele-operation company and AGV company will work together to enhance the driving performance and allow customers to operate the remote driving.</p>	<p>Port authorities and port terminals.</p> <p>Hauliers and transport/logistics companies that operates at the port.</p>



<p>Tele-operation driving implementation company is needed to configure and supervise the tele-operation driving AGV performance.</p> <p>AGV company is needed to configure the AGV to allow the port operation and evaluate the performance.</p> <p>Data protection and privacy entities to ensure the security and privacy of data.</p>	<p>Ensuring that the 5G coverage comply with the KPI.</p> <p>End-to-End tele-operation driving communications data path.</p> <p>Data recompilation from tele-operation and coverage in order to accomplish the QoS.</p>	<p>professional robot operator in every industrial area, enabling the capacity of driving several AGVs at different localisations.</p>	<p>Channels</p> <p>The best channel to approach customers is a marketing strategy where we could offer a free trial of the remote driving operation to show the advantages that can be exploited in the every-day works.</p>
	<p>Key Resources</p> <p>5G coverage.</p> <p>AGV provided with IoT devices available at the port.</p> <p>Immersive cockpit available provided with haptic globes, wheel, pedals, and VR glasses.</p> <p>Computational and storage resources.</p>		
<p>Cost Structure</p> <p>Procurement and installation of the 5G antenna equipment.</p> <p>Procurement and configuration of the AGV.</p> <p>Procurement and implementation of the immersive cockpit.</p>		<p>Revenue Streams</p> <p>By subscription</p> <p>Unique payment</p>	

3.3.3 TRANSPORTATION PLATFORM HEALTH MONITORING

Table 22. Business Model Canvas for the Transportation Platform Health Monitoring UC.

Key partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
<p>Infrastructure owners reduce damage to rail infrastructure due to wheel defects.</p> <p>Asset owners optimise maintenance cycles and increase uptime.</p> <p>Rail operators reduce operation costs.</p> <p>Forwarders for data Transparency</p> <p>Rail analytics for value data.</p> <p>Mobile IoT providers related to hardware and data.</p>	<p>Development of Rail-Health Edge Sensor for condition monitoring of flat spots and bearing defects</p> <p>Key Resources</p> <p>Sensor circuit design</p> <p>Edge hardware design</p> <p>Algorithm design</p> <p>Embedded software</p> <p>Mechanical design</p> <p>Cloud app design</p> <p>Testbed (lab and field)</p> <p>Test equipment design</p>	<p>Expanding rail health services from high-speed passenger rail-transport to rail goods and regional rail travel.</p> <p>Enable the optimised maintenance cycles and maintenance cost reductions.</p> <p>Enable the reduction of safety critical rail incidents</p> <p>Lower the IoT cost by a factor of 5X for rail goods compared to passenger RAIL</p> <p>Optimise edge analytics for rail goods</p>	<p>Relationships created with the costumers</p> <p>Channels</p> <p>Data Customers</p> <p>VTC, DB Cargo, others</p> <p>Cloud Operators</p> <p>Nexxiot, others</p>	<p>Rail operators</p>
<p>Cost Structure</p> <p>development of test equipment and edge devices</p> <p>electronic parts, mechanical part manufacturing</p> <p>engineering resources – system, hardware, software, data engineering, data science, mechanics, testing, cloud</p>		<p>Revenue Streams</p> <p>Connected IoT devices= hardware, data, and maintenance service fees</p>		



Note that the Rail-Health, i.e., the early detection of rail carriage wheel and bearing defects, has three economic benefits:

- 1) Optimisation and possible extension of maintenance cycles: Today, a full maintenance is done every six years, regardless of the condition of wheels and bearings. Eliminating unnecessary maintenance from six to twelve years would result in cost savings of € 1000/wagon per lifetime.
- 2) Rail carriage wheel flat spots can damage the rail Infrastructure: Network operators can levy 350 € penalties on rail assets operating on flat-spots greater than 50mm in width. Prompt identification and maintenance of such defects could reduce penalty cost by 1.5% of fleet x 350€ year x 12 years lifetime = € 63 / per wagon per lifetime.
- 3) Derailments occur more frequently than one might expect: In USA alone, every two weeks a train carrying hazardous materials derails on average. At an incident cost of 5M€ per incidence. There are about 439000 tank freight cars in USA. The incident cost amount to 52 weeks per year / one derailment every other week x 5M€ per incident / 439k tank freight cars * 12 years lifetime = € 99 / per wagon per lifetime.

The total cost savings over a 12-year period assuming a 439k fleet amount to € 1000 reduced maintenance cost + € 63 reduced penalty cost + € 99 reduced incidence cost = € 1162 x 439k = € 510 million.

The equipment, Installation, and monitoring infrastructure required to achieve these cost savings are 8 sensors at 18€ per sensor per wagon (add on cost to existing telemetric location service) + 50€ Installation cost per wagon + 12€ per year IT overhead x 12 years = €338 / per wagon per lifetime. If 5% 12-year financing is added (factor 1.8) this amounts to €608 invest vs. €1162 cost savings. An ROI of 200%. For a fleet of 439k tank freight cars this amounts to €250 million in cost savings.

3.3.4 INTER-MODAL ASSET TRACKING VIA IOT AND SATELLITE

Table 23. Business Model Canvas for the Inter-modal Asset Tracking via IoT and Satellite UC.

Key partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
<p>Port authorities are needed to give access to the port infrastructure.</p> <p>Port terminals to give access to the port terminal infrastructure where trucks will enter and exit for the loading or unloading of cargo.</p> <p>Hauliers to transport cargo for performing loading or unloading operations inside the port and terminal facilities.</p> <p>Ship providers are needed to transport the cargo when the</p>	<p>Procurement of IoT sensors for measuring temperature, humidity, movement, vibration, etc.</p> <p>Procurement of iNGENIOUS shipping container.</p> <p>Development of a Smart IoT Gateway.</p> <p>Ensuring that a ship and truck will be available for trials.</p> <p>Site survey.</p> <p>Installation of sensors in the container.</p> <p>Installation of a smart IoT GW on the ship.</p>	<p>The container tracking is an essential part of the supply chain and logistics to make them more efficient. By monitoring and tracking seamlessly the container in near real-time, it allows to provide all the supply chain players and stakeholders a full traceability and to optimise the transport and the storage of containerised goods. Any event related to a container is quickly notified and is allowing efficient analytics as well as taking related decision such as new sourcing plans if needed.</p>	<p>Shipping agencies, port authorities and terminals and hauliers will ease the access to the existing data sets.</p> <p>This data will be exploited by Big Data and ML-based prediction providers.</p>	<p>Shipping agencies (COSCO Shipping Lines Spain S.A) and other actors belonging to the port community (e.g., port authorities, port terminals, hauliers, freight forwarders) that are interested in the data collected.</p> <p>Secondary customers: Insurance companies that are interested in the data for offering their services to the primary customer segments.</p>



<p>ship is sailing on the sea.</p> <p>Sensor and IoT Providers are needed to deploy sensors and IoT devices in the shipping container for collecting information on cargo tracking, cargo conditions, safety conditions, etc.</p> <p>Communication and network management entities are needed to provide the satellite, wireless and IoT connectivity when the ship is sailing on the sea and also inside the port facilities and the inland for enabling the real-time tracking and the transmission of the data collected by the IoT sensors.</p> <p>Big data analytics providers are needed to analyse and exploit the data collected by the different sensors and IoT devices.</p>	<p>Sensor communication with the smart IoT GW.</p> <p>End-to-End satellite communications path.</p> <p>Key Resources</p> <p>Data streams associated to real-time location of the cargo, condition of the cargo (temperature, humidity, movement, vibration), safety conditions (stop and bump detection, container door opening), arrival and departure of vessels, containers, trucks, etc.</p> <p>IoT devices and shipping container.</p> <p>Ship and truck to transport the container in the maritime and terrestrial segment.</p> <p>The Port of Valencia and Port of Piraeus facilities to load and unload the container to the ship.</p> <p>Wireless IoT communication modems (LoRa, Wi-Fi, 4G/5G IoT) and mobile core network.</p> <p>Smart IoT Gateway, Satellite Terminal, GEO satellite, Ku-band, Satellite uplink/downlink facilities and 5G Satellite Hub.</p>	<p>By tracking and tracing the cargo, the operator will monitor the asset movement, will record the actual routes, transit times, stationing in the facilities and congestions for every transport mode. By analysing the transit performance, the operator will take informed decisions by choosing preferred routes, carriers or even modes of transport.</p> <p>By monitoring temperature, humidity, accelerometers, and even simple contact sensors the operator will assess additional states applicable for various goods. Temperature and humidity are relevant for perishable goods and abnormal variations in the values will indicate the immediate need for maintenance in order to avoid the loss of goods. Furthermore, the accelerometer output will provide real-time indication about the integrity of the goods and abnormal variations may trigger subsequent inquiries which may conclude that an accident occurred, and intervention is required.</p> <p>Continuous contact sensors data may certify that the goods are transported securely in their containers, and nobody attempted an unauthorised access. In eventuality of a door alarm the operator will alert appointed security entities to counteract a potential illegal action.</p>	<p>Channels</p> <p>The best channel used to approach customers would be a marketing strategy by offering a free trial of the inter-modal asset tracking or organising a demonstration at different events such as the NGI Forum, IoT forum, EuCNC or MWC.</p> <p>The good position of SES, COSSP, FV and iDR in maritime, satellite and logistics industry could play a key role for engaging new customers.</p>	
<p>Cost Structure</p> <p>Procurement of iNGENIOUS container.</p> <p>Procurement and installation of IoT tracking sensors.</p> <p>Procurement of components for the development of the Smart IoT Gateway (Raspberry Pi, LoRa GW, SSD cards, LimeSDR, etc.).</p> <p>Site Survey for the Installation the Satellite Terminal and the IoT GW on the ship.</p> <p>Satellite capacity for working on the SatCube Integration.</p> <p>Satellite capacity for the real demo and for demonstrations at different events.</p> <p>Use of ship and truck for transporting the iNGENIOUS container in the maritime and terrestrial segment.</p>		<p>Revenue Streams</p> <p>Asset tracking understanding and prediction service fee charged by Big Data Analytics and ML-based prediction provides to shipping agencies, port authorities and terminals and hauliers.</p> <p>Primary revenue stream comes from managed IoT connectivity on vessels and port terminals.</p> <p>Secondary revenue from hosted edge applications on Smart IoT Gateway/ satellite hub, that will make use of the infrastructure and managed connectivity.</p>		



3.3.5 SITUATIONAL UNDERSTANDING AND PREDICTIVE MODELS IN SMART LOGISTICS SCENARIOS

Table 24. Business Model Canvas for the Situational Understanding and Predictive Models in Smart Logistics Scenarios UC.

Key partners	Key Activities	Value Propositions	Customer Relationships	Customer Segments
<p>Port authorities and port terminals are needed to give access to the port infrastructure and the data related to the arrival of vessels, containers, and trucks to the port</p> <p>Sensor and IoT providers are needed to deploy new IoT sensors and to collect new data sets related to vehicle track and trace, meteorological conditions, etc.</p> <p>Communication and network management entities to improve the wireless and IoT connectivity inside the port facilities for enabling the real-time tracking and the transmission of the data collected by the IoT sensors</p> <p>Big data analytics and ML-based prediction providers able to analyse and exploit the data collected by the different sensors and IoT devices in order to model and develop situational understanding and predictive models.</p> <p>Data protection and privacy entities to ensure the security and privacy of the data used to provide the situational understanding service.</p>	<p>Identification of data sources and understanding of the port operations.</p> <p>Ingestion and integration of existing and new data sources</p> <p>IoT sensors procurement and installation</p> <p>Exploratory data analysis and development of predictive models offline</p> <p>Data ingestion from online services and deployment of predictive models online</p> <p>Development of dashboard for visualizing the situational understanding outcomes.</p> <p>Key Resources</p> <p>Data streams associated to gate access, meteorological data, arrival and departure of vessels, containers, and trucks, etc.</p> <p>IoT devices available at the port and terminals like OCR and CCTV cameras, gate access sensors, meteorological cabins, new tracking sensors, etc.</p> <p>Platforms and systems available at the port and terminals like M2M platforms, AIS, PCS, VBS, PMIS or Port Call Scheduling Systems.</p> <p>Computational and storage resources.</p> <p>Fixed and wireless networks for connecting IoT sensors.</p>	<p>Improve situational understanding and identify the potential bottlenecks related to truck access in maritime ports and terminals.</p> <p>Reduce the truck turnaround time inside the port and terminal areas, leading to reduce the length of queues and therefore, speed up the port and terminal operations.</p> <p>Reduce the CO2 emissions related to truck access to port and terminals</p>	<p>Port authorities and terminals will ease the access to the existing data sets related to the arrival of vessels, containers, and trucks.</p> <p>This data will be exploited by Big Data and ML-based prediction providers for enhance the situational understanding and the truck access operative.</p> <p>Channels</p> <p>The best channel used to approach customers would be a marketing strategy where we could offer a free trial of the situational understanding service while giving an example of other ports where this service has been successfully implemented.</p> <p>The good position of FV, CNIT and AWA in maritime and logistics industry could play a key role for engaging new customers.</p>	<p>Port authorities and port terminals</p> <p>Hauliers and transport/logistics companies</p>
<p>Cost Structure</p> <p>Procurement and installation of IoT tracking sensors.</p> <p>Service for the integration and ingestion of existing and new data sources.</p> <p>Service for the analysis of the different data sets and the deployment of models.</p> <p>Service for the deployment of a dashboard to visualise the situational understanding and predictive outcomes.</p>		<p>Revenue Streams</p> <p>Situational Understanding and Prediction service fee charged by Big Data Analytics and ML-based prediction provides to Port Authorities and Terminals.</p>		



3.3.6 SUPPLY CHAIN ECOSYSTEM INTEGRATION

Table 25. Business Model Canvas for the Supply Chain Ecosystem Integration UC.

<p>Key partners</p> <p>M2M Platform Providers: entities providing different M2M platforms operating in different operational contexts to be integrated by means of Data Virtualisation Layer. These platforms are expected to be used as data sources.</p> <p>DLT Solution Providers: entities providing a specific solution based on DLT (IOTA, Bitcoin, Ethereum and/or Hyperledger Fabric). They also provide the access to their test networks using a given interface for immutable data storage and distribution.</p> <p>Cross-M2M layer provider: entity providing a custom solution for the implementation of the cross-M2M interoperability layer based on the data virtualisation approach for the M2M platforms integration.</p> <p>Cross-DLT layer provider: entity providing a solution for the implementation of the cross-DLT interoperability layer based on TrustOS allowing end users to communicate with the underlying DLTs for immutable data storage.</p> <p>Port authorities: as end users, these entities will assess the prototype implementation in order to check whether user requirements are met according to their initial needs.</p> <p>Cybersecurity expert: entity providing privacy functions to be integrated with the main architecture in order to make sure that personal data management is in line with GDPR constraints.</p>	<p>Key Activities</p> <p>Deployment of M2M platforms in different scenarios in order to feed the interoperable layer with data relevant for the maritime events' definition.</p> <p>Aggregation of collected data at data virtualisation level and data sharing with the cross-DLT layer for secure data storage and its immutability.</p> <p>Data hash is then stored in different DLTs according to their own capabilities. Hash storage is a minimum requirement.</p> <p>End users visualise data related to events they are part of by means of an interface.</p>	<p>Value Propositions</p> <p>Interact with different available DLTs from a single access point and by means of unified API.</p> <p>Provide a single access point as well as a virtual access to heterogeneous M2M platforms and external systems in order to aggregate data relevant for the maritime events definition (e.g. GateIn, GateOut, Vessel Arrival and Vessel Departure).</p> <p>Exploit DLTs' capabilities in terms of proofs of existence and immutability of the Final Users data/events in maritime domain, according to their own needs.</p> <p>Provide dispute resolution mechanism between supply chain actors, based on the exploitation of the smart contracts.</p>	<p>Customer Relationships</p> <p>Co-creation based relationship with customers in order to allow them being involved into the design process so that according to their feedback the proposed solution can be further improved.</p>	<p>Customer Segments</p> <p>Port authorities, container terminal operators, freight forwarders, shipping companies.</p> <p>Any other operator/actor from the supply chain ecosystem interested in getting the visibility over their own assets.</p>
<p>Cost Structure</p> <p>Research and development activities (PMs).</p> <p>Licensing of software components such as SQL Server and/or Windows OS according to available computational resources and required architectural components' instantiation.</p> <p>Maintenance of existing ICT infrastructure, allowing service to be up and running.</p>	<p>Revenue Streams</p> <p>Data monetisation.</p>			
<p>Key Resources</p> <p>Computational resources for the local instantiation and deployment of the architectural components (cross-M2M and cross-DLT layers).</p> <p>M2M instances operating and collecting data in the maritime context.</p> <p>DLT instances for secure data storage according to aggregated data coming from data virtualisation layer.</p> <p>Instance of the pseudonymisation function for personal data detection and its management according to the policies from GDPR.</p>	<p>Channels</p> <p>Partners' social media channels-</p> <p>Journal submission and publications.</p> <p>Presentation and demonstration at relevant events and/or forums.</p>			



4 Conclusion

This document has provided a general overview of the regulatory framework that encloses the project and described the potential business models that IoT technologies could bring to the consortium. Special focus has been put on the regulatory aspects, since a more elaborated discussion around potential business models and future opportunities will be handled in D2.5 as a separate contribution.

D2.3 has compiled the local, national and EU information on the project area, ensuring specifically that the project propositions are compliant with the context in all application domains. This is key for demonstrating the proposed use cases in real scenarios. The deliverable has analysed these aspects from a generic perspective but has also described both regulatory and business aspects concerning each of the six use cases in iNGENIOUS. This will permit the partners involved to better fit their needs and understand the framework where their products and services may be deployed.

4.1 Regulatory Framework

The first regulatory aspect explored in this deliverable is spectrum. The document has defined the **frequency bands** that can be used with the technologies considered in the regions where the use cases are taking place. D2.3 has also explored the different alternatives that exist for deploying a specific technology.

- **Licensed spectrum** devices operate within the portion of the radio spectrum that has been designated by international, national, or local regulators to be reserved for organisations that have been granted licenses (mobile/satellite operators, verticals, etc.). Technologies such as 5G, NB-IoT or satellite communications are associated to this type of licensing. Licensed spectrum can be in turn permanent, which permits regular access to spectrum by the licensee; or temporary (spectrum leasing), where spectrum is reserved for a specific event or service.
- On the other hand, **unlicensed spectrum** is related to the frequency bands assigned to every citizen for non-exclusive usage, thus avoiding regulatory constraints. Examples of unlicensed technologies are Sigfox, LoRa or WiFi.
- **Spectrum sharing** arises as a potential solution to use spectrum bands when they are not being used in some areas and/or time slots. In this sense, LSA can be used so incumbent licence holders sub-license spectrum to others.

The deliverable has additionally explored the different requirements and limitations for **network deployments**. We have discussed the different procedures to obtain the authorisation to install a mobile station, as well as the rules to deploy a 5G core. Another topic explored was the use of maximum transmission power levels, which naturally affects those use cases where a new deployment will take place.



The document not only has tackled network regulatory aspects, but also has paid attention to **security** concerns. In here, we have provided a complete description of the NIS directive, a regulation that is the result of shared effort of the European Committee and member states of the EU to provide a first version of the EU-wide cybersecurity legislation. **Privacy** and **data protection** aspects have been also presented, with a comprehensive description of the GDPR legislation, which handles the protection of individuals about the processing of personal data.

The use of **cryptocurrencies** as part of the project, whose regulation is continuously and actively changing, has been also analysed.

4.2 Business Models

D2.3 has also identified and provided a first analysis of the current business models at strategic level that can leverage the iNGENIOUS products and services. This has been done by discussing economic concerns (how the project results are sustainable and create value); component considerations (how business is done) and strategic outcomes (design of key interdependent systems that create and sustain a competitive business).

To provide some context, the document has first provided a **PESTEL analysis**, where the different political, economic, social, technological, environmental, and legal aspects indirectly affecting the project are discussed.

Once the context has been defined, the document tackles the **technological enablers** that may bring to the consortium new business models and opportunities.

- Project partners have discussed in the detail the specific types of **non-public networks**. NPNs may be deployed as standalone NPNs (SNPN), where there is an NPN operator, and all network functions are located inside the logical perimeter of the defined premises; but they can also be considered as public network integrated NPNs (PNI-NPN). In this second alternative a non-public network is deployed with the support of a PLMN, using network slices or CAG cells, or even a combination of both. The different advantages of using such types of networks have been widely described in this document.
- **Network slicing** has been also identified as a key enabler for IoT, since it permits to fulfil a specific set of requirements that are vital for end users. The different types of business that network slicing may bring (B2B, B2C, B2B2B) have been described in this document.
- Since the project is using multiple DLT technologies such as Bitcoin or Ethereum, we have also introduced the business alternatives that they could bring. **Cryptocurrencies** are new phenomena that has not only technological implications, but also political, economic, and social, with potential impact on the environment.
- Other aspects such as the use of a **flexible RAN** for NPNs or **tactile applications** have been also introduced.



Annex A: Checklist for personal data

Table 26. GDPR checklist for personal data.

Protection of personal data	YES/NO	Information to be provided	Documents to be provided
Does your research involve processing of personal data?	<input type="checkbox"/> / <input type="checkbox"/>	<ol style="list-style-type: none"> 1) Details of the technical and organisational measures to safeguard the rights of the research participants. For instance: <ul style="list-style-type: none"> • For organisations that must appoint a DPO under the GDPR: Involvement of the DPO and disclosure of the contact details to the research participants. • For all other organisations: Details of the data protection policy for the project (i.e., project-specific, not general). 2) Details of the informed consent procedures. 3) Details of the security measures to prevent unauthorised access to personal data. 4) How is all the processed data relevant and limited to the purposes of the project ('data minimisation' principle)? Explain. 5) Details of the anonymisation /pseudonymisation techniques. 6) Justification of why research data will not be anonymised/ pseudonymised (if relevant). 7) Details of the data transfers (type of data transferred and country to which it is transferred – for both EU and non-EU countries). 	Informed consent forms + information sheets used (if relevant).
If YES: Does it involve the processing of special categories of personal data (i.e., genetic, health, sexual lifestyle, ethnicity, political opinion, religious or philosophical conviction.)?	<input type="checkbox"/> / <input type="checkbox"/>	<ol style="list-style-type: none"> 1) Justification for the processing of special categories of personal data. 2) Why can the research objectives not be reached by processing anonymised/ pseudonymised data (if applicable)? 	
Does it involve processing of genetic, biometric or health data?	<input type="checkbox"/> / <input type="checkbox"/>	-	Declaration confirming compliance with the laws of the country where the data was collected
Does it involve profiling, systematic monitoring of individuals or processing of large scale of special categories of data, intrusive methods of data processing (such as, tracking, surveillance, audio and video recording, geolocation tracking etc.) or any other data processing operation that may result in high risk to the rights and freedoms of the research participants?	<input type="checkbox"/> / <input type="checkbox"/>	<ol style="list-style-type: none"> 1) Details of the methods used for tracking, surveillance, or observation of participants. 2) Details of the methods used for profiling. 3) Risk assessment for the data processing activities. 4) How will harm be prevented, and the rights of the research participants safeguarded? Explain. 5) Details on the procedures for informing the research participants about profiling, and its possible consequences and the protection measures. 	Opinion of the data controller on the need for a data protection impact assessment (art.35 GDPR) (if relevant).



<p>Does your research involve further processing of previously collected personal data (including use of pre-existing data sets or sources, merging existing data sets)?</p>	<p>□ / □</p>	<ol style="list-style-type: none"> 1) Details of the database used or of the source of the data. 2) Details of the data processing operations. 3) How will the rights of the research participants be safeguarded? Explain. 4) How is all the processed data relevant and limited to the purposes of the project ('data minimisation' principle)? Explain. 5) Justification of why the research data will not be anonymised/ pseudonymised (if relevant). 	<ol style="list-style-type: none"> 1) Declaration confirming lawful basis for the data processing. 2) Permission by the owner/manager of the data sets (e.g. social media databases) (if applicable). 3) Informed Consent Forms + Information Sheets + other consent documents (opt in processes, etc.). (if applicable).
<p>Does your research involve publicly available data?</p>	<p>□ / □</p>	<p>Confirm that the data used in the project is publicly available and can be freely used for the project.</p>	<p>Confirm that the data used in the project is publicly available and can be freely used for the project.</p>
<p>Is it planned to export personal data from the EU to non-EU countries? Specify the type of personal data and countries involved</p>	<p>□ / □</p>	<p>Details of the types of personal data to be exported. How will the rights of the research participants be safeguarded? Explain</p>	<p>Declaration of confirming compliance with Chapter V of the GDPR.</p>
<p>Is it planned to import personal data from non-EU countries into the EU? Specify the type of personal data and countries involved</p>	<p>□ / □</p>	<p>Details of the types of personal data to be imported.</p>	<p>Declaration confirming compliance with the laws of the country in which the data was collected.</p>

Note: Pseudonymisation and anonymisation are different concepts. 'Anonymised' means that the data has been rendered anonymous in such a way that the data subject can no longer be identified (and therefore is no longer personal data and thus outside the scope of data protection law). 'Pseudonymised' means to divide the data from its direct identifiers so that linkage to a person is only possible with additional information that is held separately. The additional information must be kept separately and securely from processed data to ensure non-attribution.



References

- [1] ITU-R, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," Recommendation ITU-R M.2083-0, 2015.
- [2] 3GPP, "NR; Base Station (BS) radio transmission and reception," TS 36.104, v17.1.0, 2021.
- [3] 3GPP, "Evolved universal terrestrial radio access (E-UTRA); base station (BS) radio transmission and reception," TS 36.104, v17.1.0, 2021.
- [4] 3GPP, "Base station (BS) radio transmission and reception (FDD)," TS 25.104, v16.0.0, 2019.
- [5] GSMA, "Spectrum Sharing," June 2021.
- [6] M. D. Mueck, V. Frascolla and B. Badic, "Licensed shared access — State-of-the-art and current challenges," *1st International Workshop on Cognitive Cellular Systems (CCS)*, 2014.
- [7] Qualcomm, "Global update on spectrum for 4G & 5G," December 2020.
- [8] GSMA, "5G Spectrum," GSMA Public Policy Position, March 2021.
- [9] 3GPP, "First 5G NR specs Press release," December 2017.
- [10] 3GPP, "Technical specification group radio access network; NR; user equipment (UE) radio transmission and reception," TS 38.101, v17.1.0, 2021.
- [11] Ericsson, "5G spectrum for local industrial networks," Whitepaper.
- [12] 3GPP, "Study on enhancement of 5G System (5GS) for vertical and Local Area Network (LAN) services," TR 23.734.
- [13] 3GPP, "Study on management of Non-Public Networks (NPN)," TR 28.807.
- [14] 3GPP, "SID on NR Industrial IoT," RP-181479, 2018.
- [15] Ericsson, "How 5G integrates with TSN-based industrial communication systems," February 2021.
- [16] X. Lin, S. Rommer, S. Euler, E. A. Yavuz and R. S. Karlsson, "5G from Space: An Overview of 3GPP Non-Terrestrial Networks," 2021.
- [17] 3GPP, "Work Item on "Guidelines for extra-territorial 5G systems"," SP-191042.
- [18] 3GPP, "Guidelines for extra-territorial 5G Systems (5GS)," TR 22.926 V0.3.0, April 2021.
- [19] European Commission, "Mandate to CEPT to develop harmonised technical conditions for spectrum use in support of the introduction of next-generation (5G) terrestrial wireless systems in the Union," December 2016.
- [20] Spain government, "National Table of Frequency Allocation (CNAF)".
- [21] Camera dei deputati, 2018. [Online]. Available: https://www.camera.it/leg17/465?tema=la_gestione_delle_frequenze_e_lo_spettro_radio#m.
- [22] "sull'uso attuale e futuro del sistema mobile di seconda generazione GSM e di quello di terza generazione UMTS," [Online]. Available: https://www.mise.gov.it/images/stories/documenti/Consultazione_sutecnologia2G_3G_2020_.pdf.



- [23] Camera dei deputati, “Spettro radio, 5G ed innovazione tecnologica,” April 2021. [Online]. Available: <https://www.camera.it/temiap/documentazione/temi/pdf/1105154.pdf>.
- [24] Gazzetta ufficiale della Repubblica Italiana, «Decreto legislativo n.259: Codice delle comunicazioni elettroniche,» August 2003.
- [25] Italian Regulation, «Decree of the President of the Council of Ministers: Establishment of exposure limits, attention values, and quality goals to protect the population against electric, magnetic, and electromagnetic fields generated at frequencies between 100kHz and 300GH,» 8 July 2003.
- [26] Boletín Oficial del Estado, «Ley 9/2014, de 9 de mayo, General de Telecomunicaciones,» May 2014.
- [27] BOE, «Real Decreto 1066/2001,» September 2001.
- [28] European Parliament, «Regulation (EU) 2016/679 of the European Parliament and of the Council,» April 2016.
- [29] International Organization for Standardization, «ISO 31000:2018, Risk management - Guidelines,» February 2018.
- [30] “GDPR Enforcement Tracker,” [Online]. Available: <https://www.enforcementtracker.com/>.
- [31] “GDPR,” [Online]. Available: <https://www.garanteprivacy.it/home/footer/link>.
- [32] European Commission, «Blockchain Strategy,» November 2021.
- [33] European Commission, «Daily News,» 14 07 2021. [En línea]. Available: https://ec.europa.eu/commission/presscorner/detail/en/mex_21_3703.
- [34] European Central Bank, “Digital euro report,” October 2020. [Online]. Available: <https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr201002~f90bfc94a8.en.html>.
- [35] European Central Bank, “Public consultation on a digital euro,” April 2021. [Online]. Available: <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210414~ca3013c852.en.html>.
- [36] European Central Bank, “Launch of digital euro project,” July 2021. [Online]. Available: <https://www.ecb.europa.eu/press/pr/date/2021/html/ecb.pr210714~d99198ea23.en.html>.
- [37] European Union, “Directive (EU) 2018/843,” May 2018.
- [38] CJEU, “CJEU states that Bitcoin is a virtual currency whose exchange for traditional currencies is exempt from VAT,” October 2015. [Online]. Available: <https://curia.europa.eu/juris/document/document.jsf?docid=170305&text=&dir=&doclang=EN&part=1&occ=first&mode=DOC&pageIndex=0&cid=11910576>.
- [39] European Union, “Summary of the Opinion of the European Data Protection Supervisor on the Proposal for a Council Regulation on the establishment and operation of an evaluation and monitoring mechanism to verify the application of the Schengen acquis”.
- [40] European Union, “EDPS Opinion on the Proposal for a Regulation on Markets in Crypto-assets, and amending Directive (EU) 2019/1937”.



- [41] European Union, “Opinion of the European Central Bank of 28 April 2021 on a proposal for a regulation of the European Parliament and of the Council on a pilot regime for market infrastructures based on distributed ledger technology (CON/2021/15) 2021/C 244/04,” April 2021.
- [42] United Nations, «Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to Automated Lane Keeping System,» Economic and Social Council, June 2020.
- [43] European Union, “Countries,” [Online]. Available: https://europa.eu/european-union/about-eu/countries_en.
- [44] European Commission, “Recovery plan for Europe,” [Online]. Available: https://ec.europa.eu/info/strategy/recovery-plan-europe_en.
- [45] European Commission, “EU Vaccines Strategy,” [Online]. Available: https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/public-health/eu-vaccines-strategy_en.
- [46] European Parliament, “EU-US Relations,” [Online]. Available: <https://www.europarl.europa.eu/unitedstates/en/eu-us-relations>.
- [47] European Commission, “United States - Trade,” [Online]. Available: <https://ec.europa.eu/trade/policy/countries-and-regions/countries/united-states/>.
- [48] M. Kaeding, J. Pollak and P. Schmidt, Euroscepticism and the future of Europe: views from the capitals.
- [49] European Council, “EU migration policy,” [Online]. Available: <https://www.consilium.europa.eu/en/policies/eu-migration-policy/>.
- [50] Eurostat, “GDP and main components (output, expenditure and income),” [Online]. Available: https://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=nama_10_gdp&lang=en.
- [51] Eurostat, “Economy COVID-19,” [Online]. Available: <https://ec.europa.eu/eurostat/web/covid-19/economy>.
- [52] FRED Economic Data, “Gross Domestic Product for European Union (27 countries from 2020),” [Online]. Available: <https://fred.stlouisfed.org/series/CPMNACSCAB1GQEU272020>.
- [53] European Union, “Countries of the EU,” [Online]. Available: https://europa.eu/european-union/about-eu/countries_en.
- [54] European Central Bank, “International use of the euro broadly stable in 2020,” June 2021.
- [55] European Central Bank, “US dollar (USD) exchange rate,” [Online]. Available: https://www.ecb.europa.eu/stats/policy_and_exchange_rates/euro_reference_exchange_rates/html/eurofxref-graph-usd.en.html.
- [56] European Commission, “Horizon 2020 (H2020) programme,” [Online]. Available: <https://ec.europa.eu/programmes/horizon2020/en/home>.
- [57] European Commission, “Horizon Europe programme,” [Online]. Available: https://ec.europa.eu/info/research-and-innovation/funding/funding-opportunities/funding-programmes-and-open-calls/horizon-europe_en.
- [58] B. Hall and B. Khan, “Adoption of New Technology,” 2004.



- [59] Mckinsey Global Institute, “Innovation in Europe - Changing the game to regain a competitive edge,” October 2019.
- [60] European Commission, “Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses,” January 2017.
- [61] European Union, “Living in the EU,” [Online]. Available: https://europa.eu/european-union/about-eu/figures/living_en.
- [62] Central Intelligence Agency (CIA), «The world factbook - European Union,» 2021.
- [63] The Atlantic, “How Airline Ticket Prices Fell 50 Percent in 30 Years (And Why Nobody Noticed),” February 2013.
- [64] European Commission, “Schengen Area,” [Online]. Available: https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/schengen-area_en.
- [65] Transportation Security Administration, “TSA checkpoint travel numbers (current year versus prior year(s)/same weekday),” [Online]. Available: <https://www.tsa.gov/coronavirus/passenger-throughput>.
- [66] Eurocontrol, “COVID-19 impact on the European air traffic network,” [Online]. Available: <https://www.eurocontrol.int/covid19>.
- [67] European Commission, “Telework in the EU before and after the COVID-19: where we were, where we head to”.
- [68] “5GPPP homepage,” [Online]. Available: <https://5g-ppp.eu/>.
- [69] Next-Generation IoT, «Official website,» [En línea]. Available: <https://www.ngiot.eu/>.
- [70] I. Lorenzoni and N. Pidgeon, “Public Views on Climate Change: European and USA Perspectives,” *Climatic Change* 77, 73–95, 2006.
- [71] European Commission, “A European Green Deal,” [Online]. Available: https://ec.europa.eu/info/strategy/priorities-2019-2024/european-green-deal_en.
- [72] European Commision, “Intellectual property rights,” [Online]. Available: https://ec.europa.eu/info/business-economy-euro/doing-business-eu/intellectual-property-rights_en.
- [73] Research and Markets, “United States Private LTE & 5G Network Market Size, Share & Trends Analysis Report 2020-2027,” September 2020.
- [74] R. Sharma, «Private LTE and 5G Market to Triple to \$10B by 2025, says Mobile Experts,» *The Fast Mode*, 20 February 2020.
- [75] 3GPP TR 22.830 v16.1.0, «Study on business role models for network slicing,» December 2018.
- [76] I. Demartino, “Vitalik Buterin Speaks About the Ethereum Foundation, Proof-of-Stake and More,” *Coinjournal*, 26 October 2015.
- [77] T. Erdbrink, “How Bitcoin Could Help Iran Undermine U.S. Sanctions,” *The New Yourk Times*, 29 January 2019.
- [78] M. Mavadiya, “Putin And Ethereum: A Match Made In Fintech,” *Forbes*, 29 August 2017.
- [79] The World Bank, “Financial Inclusion,” October 2018.
- [80] L. Shin, “How Bitcoin Solved This Serial Entrepreneur's Problems,” *Forbes*, 8 August 2017.



- [81] “Venezuelans try to beat hyperinflation with cryptocurrency revolution”.*DW*.
- [82] D. Leigh and R. Evans, “WikiLeaks says funding has been blocked after government blacklisting,” *The Guardian*, 14 October 2010.
- [83] R. Huang, “How Bitcoin And WikiLeaks Saved Each Other,” *Forbes*, 26 April 2019.
- [84] P. H. Madore, “‘Alt-Right Twitter’ Gab Moves to Bitcoin Payments Due to Banking Blacklist,” *Yahoo! finance*, 26 November 2018.
- [85] K. Martin and B. Nauman, “Bitcoin’s growing energy problem: ‘It’s a dirty currency’,” *Financial Times*, 20 May 2021.
- [86] J. Wiczner, “Jack Dorsey Says Bitcoin Can Make the World Greener. Could He Be Right?,” *Intelligencer*, 20 May 2021.
- [87] C. Martin, “Bitcoin Miner Is Scoring 700% Profits Selling Energy to Grid,” *Bloomerang*, 1 October 2020.

