NEXT
GENERATION
INTERNET

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

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

inGenious

D2.2 System and Architecture Integration (Initial)

Revision: v1.0

Work package	WP 2
Task	Task 2.2
Due date	30/11/2021
Submission date	30/11/2021
Deliverable lead	Barkhausen Institut (BI)
Version	1.0
Authors	Ahmad Nimr (TUD), Alexandr Tardo (CNIT), Carlos Alcaide Pastrana (TID), Carsten Weinhold (BI), Christos Politis (SES), Clemens Saur (NCG), Cosimo Zotti (TEI), Efstathios Katranaras (SEQ), Erin Seder (NXW)), Francisco Nieto (NED, Giacomo Bernini (NXW), Gino Ciccone (TEI), Giuseppina Carpentieri (TEI), Guillaume Vivier (SEQ), Ignacio Benito Frontelo (NOK), Ignacio J. Garcia Zuazola (NOK), Jaime Ruiz (NOK), Javier Renart (UPV), Joe Cahill (iDR), Jose Costa-Requena (CMC), José Luis Cárcel (FV), Juan Jose Garrido Serrato (SES), Julian Campo Sayes (ASTI), Jussi Poikonen (AWA), Manuel Fuentes (5CMM), Miguel Cantero (5CMM), Pietro Piscione (NXW), Tadeusz Puźniakowski (PJATK)
Reviewers	Nuria Molner (UPV), José Luis Cárcel (FV), Joshwa Pohlmann (BI), Michael Roitzsch (BI), Marek Bednarczyk (PJATK), Efstathios Katranaras (SEQ), Jussi Poikonen (AWA), Gino Ciccone (TEI), Javier Renart (UPV), Ahmad Nimr (TUD)

Abstract	This document provides an overview of the iNGENIOUS cross-layer architecture. The main purpose of this deliverable is to reach a common understanding of the project at a technical level among all consortium partners and those supporting the project from outside.
Keywords	INGENIOUS, architecture, vertical, cross-layer

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	30/11/2021	Public version of deliverable D2.2	See author list

Disclaimer

This iNGENIOUS D2.2 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

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

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

DEM: Demonstrator, pilot, prototype, plan designs

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

OTHER: Software, technical diagram, etc.

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

Executive Summary

This document describes the iNGENIOUS cross-layer architecture, which is the subject of task T2.2 in the project work plan. While many aspects of the architecture have already been defined during the proposal phase, some requirements and interrelations did not become clear until the technical work had started. Based on the full definition of the six use cases in *D2.1 Use cases, KPIs, and requirements*, all partners described already in month M6 the technologies and components they intended to contribute to the project. That early milestone version of this document served as a point of reference to establish a common understanding among all iNGENIOUS partners. Now, roughly one year into the project, this updated version of D2.2 offers to the consortium and external parties a refined view on the iNGENIOUS architecture and a comprehensive description of all technological building blocks.

This document first describes the architecture from a high-level point of view, which also points out how iNGENIOUS aims to address the challenges posed by the use cases. The four chapters that follow, one for each layer of the architecture, will then cover in detail all the components and how they work together to realize the next-generation supply chain. The individual partner contributions, the key innovations, and their relevance to the project's use cases are highlighted on a per-component basis.

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

Table of Contents

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

List of Figures

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

Abbreviations

AGV	Automatic Guided Vehicle
AI	Artificial Intelligence
API	Application Programming Interface
CPU	Central Processing Unit
DFT	Discrete Fourier Transform
DLT	Distributed Ledger Technology
DRX	Discontinuous Reception
DVL	Data Virtualisation Layer
eMBB	Enhanced Mobile Broadband
eMTC	Enhanced Machine Type Communication
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
FDD	Frequency Division Multiplex
FPGA	Field Programmable Gate Array
GDPR	General Data Protection Regulation
gNB	Next Generation NodeB
GSMA	GSM (Groupe Speciale Mobile) Association
GW	Gateway
HTTP	Hypertext Transfer Protocol
ID	Identification
IEEE	Institute of Electrical and Electronics Engineers
IMT	International Mobile Telecommunications
IoT	Internet of Things
IOTA	Internet of Things Association
IP	Internet Protocol
IQ	Inverse Quantization
IT	Information Technology
LPWA	Low-Range Low-Power Wide Area
LTE	Long Term Evolution
MAC	Medium Access Control
MANO	Management and Network Orchestration
MEC	Multi-access Edge Computing
ML	Machine Learning
mMTC	Massive Machine Type Communication
MQTT	MQ Telemetry Transport
MR	Mixed Reality
MTC	Machine Type Communication

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

NB	Narrow Band
NFV	Network Function Virtualization
NG	Next Generation
NR	New Radio
NSA	Non-Standalone
NTN	Non-Terrestrial Networks
OS	Operating System
OSI	Open Systems Interconnection
PDCCH	Physical Downlink Control Channel
PHY	Physical Layer
RAN	Radio Access Network
RAT	Radio Access Technology
RF	Radio Frequency
RRC	Radio Resource Control
RRM	Radio Resource Management
SA	Standalone
SDN	Software-Defined Networking
SPI	Serial Peripheral Interface
TCU	Trusted Communication Unit
TLS	Transport Layer Security
UDP	User Datagram Protocol
UE	User Equipment
URLLC	Ultra-Reliable Low Latency Communication

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

1 Introduction

The iNGENIOUS cross-layer architecture is derived from the functional and non-functional requirements that have been identified within the six use cases of the project. They are described in detail in deliverable *D2.1 Use cases, KPIs, and requirements* [1], but a summary of what they cover will be given here.

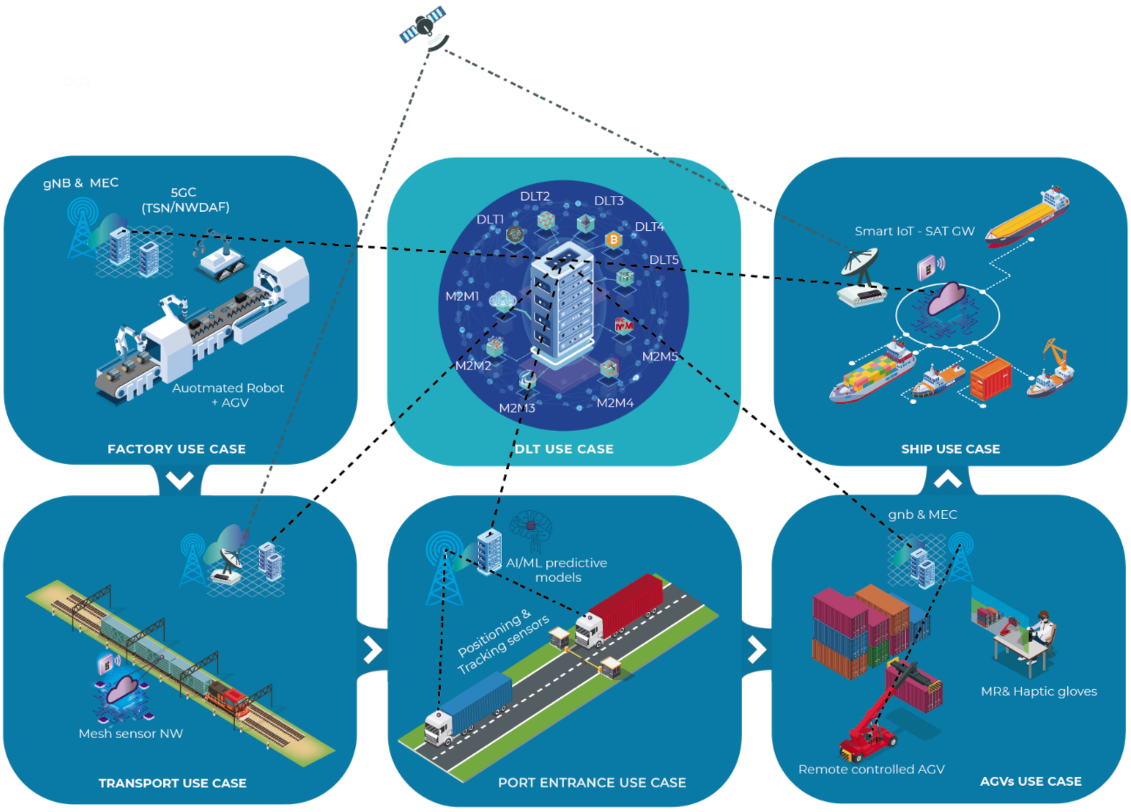


Figure 1.1: The six use cases of the iNGENIOUS project covering the supply chain and data management.

The principal approach of the iNGENIOUS project is to build the next-generation supply chain by exploiting the wealth of data that Internet of Things (IoT) technology can provide. As shown in Figure 1.1, the iNGENIOUS use cases start right in manufacturing (*Factory* use case), where automated robots increase efficiency by working fully autonomously or by assisting human workers. To innovate logistics, IoT sensors shall monitor the safety-critical parts of land-based transport vehicles, thereby enabling longer maintenance intervals to reduce costs and ensuring reliable detection of defects that could otherwise lead to accidents (*Transport* use case). By integrating network technologies ranging from local-area wireless networks all the way up to satellites, the project aims to enable in the *Transport* and, ultimately, the *Ship* use case a comprehensive tracking of assets in shipping containers across land and sea. To improve port operations in the *Port Entrance* use case, iNGENIOUS seeks to develop tools for optimizing container loading and unloading in ports by minimizing truck turnaround times. The project partners also exploit and enhance

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

5G networks to remotely control vehicles in situations where humans would be in danger or exposed to adverse environmental conditions (*AGV* use case). The *DVL/Cross-DLT* use case aims to integrate the various data flows into a comprehensive data management and analytics framework, while providing important functionality for securing supply-chain data.

Key principles to enable these use cases are:

1) Real-time positioning and tracking of physical goods in factory, logistics, and port environments through novel IoT devices with low energy consumption
2) Low-latency and reliable communication between sensors, controllers, and actuators in factory and port scenarios
3) Ability to access all data streams linked to operational processes in logistics and supply-chain data networks

The data-accessibility challenge, and the security and privacy requirements associated with it, require a system architecture where technologies from many stakeholders are integrated across all layers. The same is true for real-time positioning and time-critical communication links between IoT-enabled machinery and edge components to minimize latency. The architecture to support the iNGENIOUS approach must therefore be a true cross-layer architecture and well understood by all project partners.

The architecture described in this document, especially the component interactions and dependencies, represents the “ideal” iNGENIOUS cross-layer architecture as envisioned by the consortium. It is therefore a superset of the architectural components considered within the six use cases. Thus, these subsets may include simplifications compared to the complete architecture in order to make demonstrations practical. Nevertheless, this deliverable shall serve as a common point of reference for all technical activities in the work packages, ensuring that individual components fit their purpose in the overall system.

Chapter 2 consists of a high-level description of the architecture. Chapter 3 covers all components of the things layer that are subject of the research in WP3 of the project. Chapter 4 describes the network layer from WP4. Components in the data management layer are described in Chapter 5, followed by Applications and Data Analytics in Chapter 6. Both of these chapters cover WP5. Chapter 7 concludes this document.

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

2 Architecture Overview

The iNGENIOUS architecture consists of four layers. The first three layers range from low-level hardware over heterogeneous networks to data management and analytics services. A fourth layer on top hosts applications that rely on the services provided by iNGENIOUS components underneath.

The "things" layer at the bottom of the iNGENIOUS architecture includes all Internet of Things (IoT) devices, such as sensors and actuators. These devices interact with the physical world in static and mobility conditions (e.g., because they are part of a vehicle or attached to a shipping container). Sensors and actuators require embedded computers and network communication hardware to become IoT devices. These information-technology components are part of the bottom layer as well and the latter (e.g., wireless modems) are right at the boundary to the network layer.

Most "thing" components are only needed for specific use cases, but representatives of generic classes such as sensors or actuators are always present. Figure 2.1 shows an instantiation of the things layer with IoT devices relevant to all iNGENIOUS use cases (i.e., factory, transport, port entrance, AGV, and ship use cases).

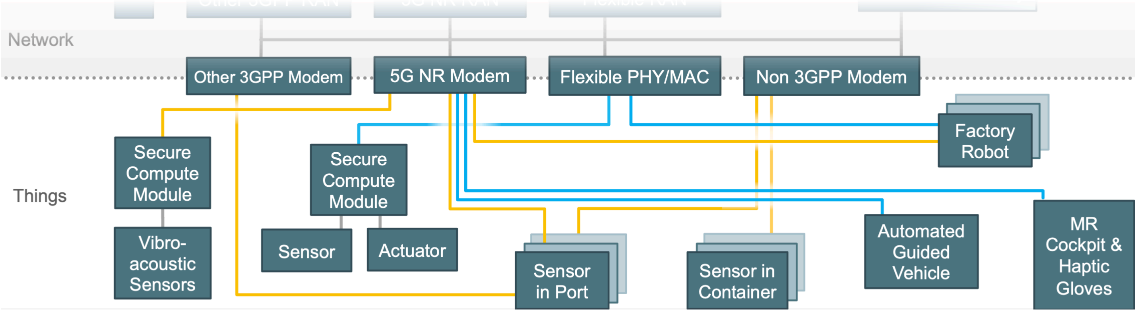


Figure 2.1: IoT devices in the iNGENIOUS architecture for all use cases considered in the project.

As IoT devices serve many different and very diverse purposes, there is no one-size-fits-all solution for connecting them to a network. For those that operate in a fixed location it may be practical to use wired connections, but most of them – especially those needed in logistics scenarios – require wireless connections. Depending on the device type, energy constraints, and operating environments, different radio technologies need to be used. Hence, the iNGENIOUS architecture must support heterogeneous networks to cover a multi-dimensional space of bandwidth, latency, range, reliability, and energy-efficiency demands. Figure 2.2 shows the iNGENIOUS network layer, which includes 3GPP-compliant technologies such as Cellular IoT and 5G networks. This layer also includes non-3GPP networks, some of which are integrated into the architecture via a smart IoT gateway. To support the transportation-platform health monitoring and container-shipping use cases, satellite connectivity is also included as a crucial component of the iNGENIOUS network layer.

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

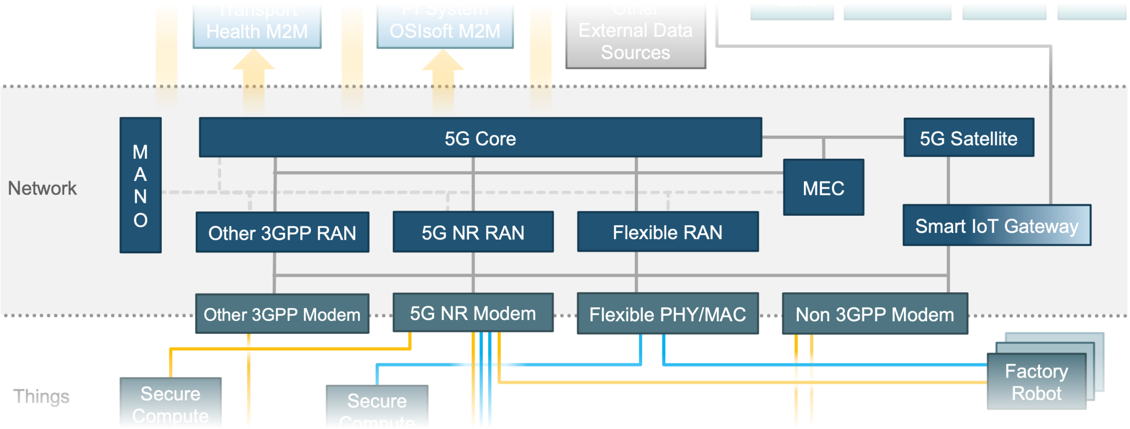


Figure 2.2: Network layer of the iNGENIOUS architecture.

IoT devices not only differ in terms of radio access technology, but they are also connected via several, incompatible machine-to-machine (M2M) platforms that serve the different stakeholders in the heterogeneous supply chain. Data flows from the IoT devices through the network layer into all these M2M silos. As shown in Figure 2.3, the iNGENIOUS Data Virtualization Layer (DVL) makes data from all M2M platforms accessible using one common interface. Thus, the DVL enables comprehensive end-to-end tracking and monitoring of all supply chain assets, as well as predictions and optimizations based on that data. The DVL also serves as the central component to ensure the integrity of all supply chain data by logging them in distributed ledger networks. Multiple Distributed Ledger Technology (DLT) systems are supported by the iNGENIOUS architecture. It is the responsibility of a Cross-DLT Layer, which relies on Telefonica's TrustOS, to virtualize the DLTs and to record securely all transactions passing through the DVL.

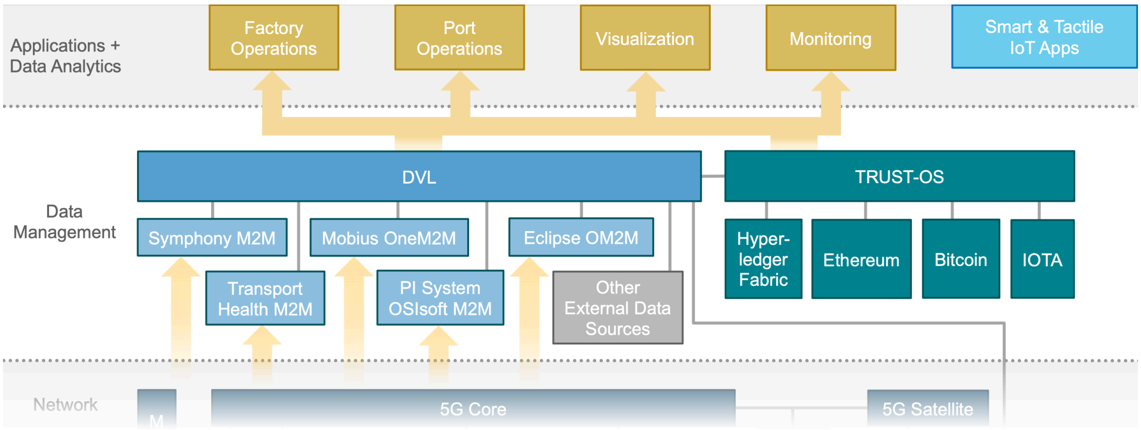


Figure 2.3: Data management and analytics layer of the iNGENIOUS architecture for applications considered in the project use cases.

To complete the architecture description, let us consider all four layers together, including the applications. The interrelationships of all components and how they cooperate is shown on the following page.

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

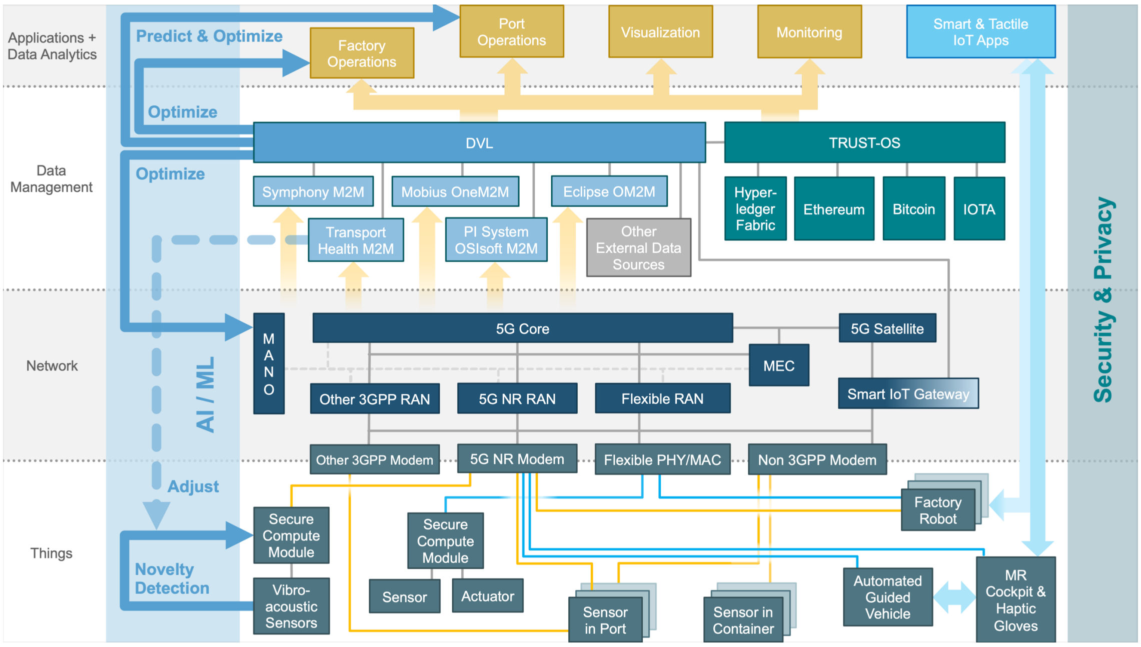


Figure 2.4: Complete iNGENIOUS architecture with all components and the interaction between them.

The yellow arrows in Figure 2.4 visualize the major flows of information from the things layer through the various M2M platforms and the DVL to the applications at the top. These data flows are security critical, which is why all this data is pseudonymized in the DVL and logged into the DLTs to ensure integrity, as well as to enable proof-of-existence of supply-chain records. However, these data flows do not require extremely low latency. In contrast, the light-blue arrows on the right side represent time-critical connections used to receive sensor readings (e.g., camera feeds) and to send control commands to actuators (e.g., robot arms). Those connections are used for remote operation of robots and automated guided vehicles in the factory and AGV use cases, respectively. Here, short and bounded response times are of critical importance. Low latency must be guaranteed by all the network components that support these connections (not highlighted in the figure for readability reasons). To minimize latency, some computations for control operations might actually run in a nearby Multi-access Edge Cloud (MEC) that is located within the network infrastructure.

Many of the innovations that iNGENIOUS aims to create are only possible because technologies from multiple layers of the architecture are combined to enable new and powerful cooperation. The first cross-layer technology in the iNGENIOUS architecture is the use of Artificial Intelligence and Machine Learning (AI/ML) that is visualized in blue arrows on the left-hand side of Figure 2.4. At the application level, ML models are trained on data that is made accessible by the DVL together with observed arrival times of sea vessels provided by external maritime port systems. To optimize port operations, the same types of DVL-provided data are then fed into these models to more accurately predict when vessels will arrive at maritime ports. In the same (i.e., Port Entrance) use case, a similar approach is applied to optimize truck turn-

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

around times in the ports. But as a cross-layer technology, AI/ML is also employed to optimize internal iNGENIOUS services, namely within the Management and Network Orchestration (MANO) component of the 5G network. Using AI/ML, MANO adapts the assignment of network resources to IoT devices at the things layer. In addition to that, ML-based data processing is used at the edge within energy-constrained IoT sensors. ML use across all layers is visualized in Figure 2.4, which shows in the bottom-left corner the vibro-acoustic sensors. These sensors are augmented with neuromorphic processing capabilities that enable the transportation-health use case.

The second cross-layer aspect of the architecture is about security and privacy. Those two security goals must be considered across all layers and a detailed discussion of both state of the art and novel measures applicable to iNGENIOUS can be found in deliverable *D5.1 Key technologies for IoT data management benchmark* [2]. The DVL plays an important role in data protection as it acts as a pseudonymization entity for all the use cases that need to handle personal data according to European General Data Protection Regulation (GDPR) directives. The cooperation between the DVL and the DLTs enables manipulation-proof recording of observed events and thus provides a critical building block to ensure data integrity across the entire supply chain. In the network layer, 5G networks incorporate security enhancements over previous 3GPP standards from which all use cases benefit. For example, in the factory use case, robots are remote controlled by smart applications running in a nearby MEC. Securing the communication links that transmit both sensor readings and actuator commands is essential to guarantee safety in automated factory operations, especially when humans are present. The security requirements are similarly obvious when regarding the remotely-operated vehicles in the AGV use case (see “Automated Guided Vehicles” and “MR-based Cockpit & Haptic Gloves” at the bottom of Figure 2.4). However, in the end, they benefit all use cases. Finally, the lowest layer plays a critical role in the iNGENIOUS security story as well. This includes carrying out policy analysis and definition for Identity & Access management for 5G-connected IoT devices. Additionally, the project will employ a novel system architecture to construct the embedded computers that connect “things” to the network, enabling cryptographic proof of the identity, integrity, and trustworthiness of both IoT devices and servers in MECs and remote data centres.

The discussion and visualizations above show that the iNGENIOUS architecture is generic and applicable to many different use cases. Most of the components in the middle layers are shared and needed in all the supply-chain scenarios we consider. Differences exist at the things layer and at the application level. This is of course expected, but there are similarities with regard to the DVL-supported data analytics techniques in the different use cases.

In the following four chapters, the components of all layers are described in greater detail and their interaction with each other is discussed. For each component, key innovations and interfaces to other building blocks of the architecture are highlighted, as well as the use cases that depend on them.

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

3 IoT Device Layer

The lowest level within the IoT system architecture is the IoT device layer, which includes the "things" that interact with the physical world. Primarily, these things are sensors and actuators. To become IoT devices and data originators, they require embedded compute units and network communication hardware that connects them securely to a network.

In terms of IoT devices and respective components, iNGENIOUS will generally consider three groups:

a. *Edge sensors*, integrated with a highly secure and low-power compute platform, and connected via a toolbox of adoptable state-of-the-art and innovative connectivity and modem solutions for optimized asset tracking and monitoring

b. *Immersive devices* such as mixed reality glasses and haptic devices for enabling the remote controlling of automated actuators in real-time with human feedback

c. *Actuators,* such as Automated Guided Vehicles (AGVs) and automated robots for logistics transportation in maritime ports and terminals or distribution in smart factories

Accordingly, iNGENIOUS will evolve the hardware and software architectures of the various components of the IoT devices as well as the connectivity solutions in order to address the current limitations and ease their adoption in the selected use cases. For the two main parts of the IoT device layer, the following aspects are considered:

- **Components:**
  - *Edge sensors* with Context-based Neuromorphic Edge Clustering for cost-optimized use-case specific system solutions
  - *Tile-based hardware/software architecture* with M^3 microkernel-based operating system with remote attestation and secure software update infrastructure in order to give the device the ability to process data locally, securely, and at low power
  - *Compact, Low-Power, and Customizable 5G modem* for flexible and "plug and play" 5G wireless connectivity experience
  - *Application aspects* that mixed-reality glasses, haptic devices and AGV-related devices should enable in order to fulfil the constrained tactile requirements of immersive use cases
- **Connectivity:**
  - *Flexible, software-defined PHY/MAC* with different flexibility level at compile-time and run-time for customization and optimization to specific IoT air interfaces as well as to support for different

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

traffic classes (e.g., enhanced mobile broadband (eMBB), ultra-reliable low latency communications (URLLC), and massive machine type communications (mMTC)

- Enhancements to lower the cost of communication (e.g., in terms of computational complexity, power consumption, latency, flexibility), leveraging improvements discussed in the standardization bodies and investigating new innovative solutions

In this chapter, we introduce the diverse IoT components and the connectivity solutions which iNGENIOUS will evolve and leverage for its use cases.

3.1 Edge Sensors

Edge Sensors will be integrated in an overall IoT infrastructure. The mission of edge sensors is to optimize the Cloud-Edge paradigm, where communication costs for offloading to the cloud are traded against cost of local computation capacity, as shown in Figure 3.1:

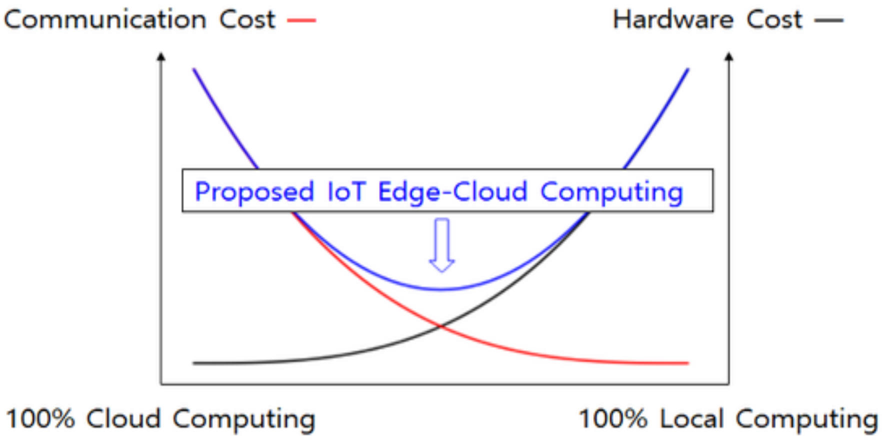


Figure 3.1: Cost for communication needed to offload vs. hardware cost for local computing

As this is closely related to the required communication load, there is not one optimal solution, but multiple use-case specific solutions exist with respect to computing power, computing energy, transmission load, and connectivity. Figure 3.1 shows the basic architectural configurations that will be considered within iNGENIOUS.

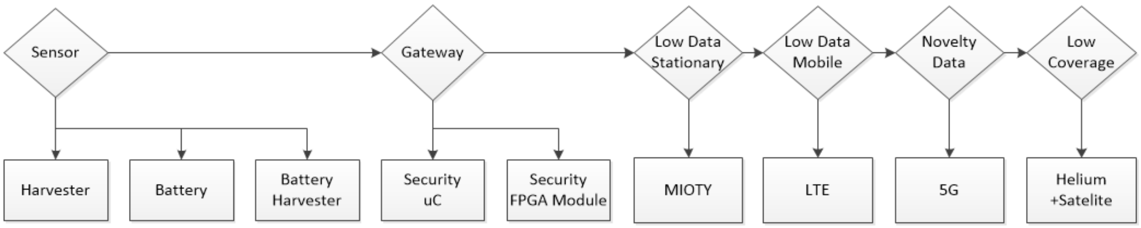


Figure 3.2: Architectural configurations for integrating edge sensors

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

A critical ingredient of Edge Computing is the data. For AI-based computations in general, and also at the edge, balanced and diverse data must be used. Design of Experiments (DoE) [3] is a good starting point for collecting data. However, DoE is expensive and rarely comprehensive. Often, there are many factors which are simply not foreseen when a DoE is conceptualized. Context-based Neuromorphic Edge Clustering is a solution to this problem. Whether used to facilitate long duration data collection, or as a small percentage of the overall edge sensor fleet, or for defect confirmation and data analysis, Context-based Neuromorphic Edge Clustering collects diversity data to facilitate and accelerate data science.

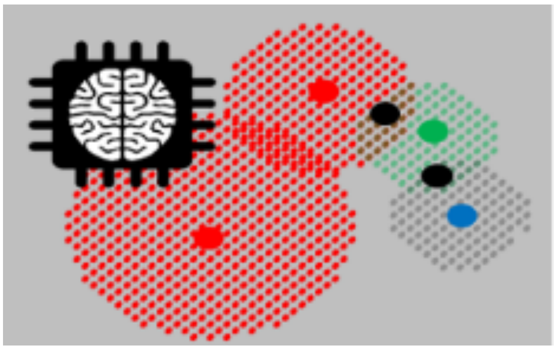


Figure 3.3: Neuromorphic Clustering (Known Clusters & Unoccupied Feature Space)

NeuroControls (NCG) will pilot the approach of edge data collection to facilitate the transportation platform health-monitoring use case. This will be in addition to a toolbox of adoptable connectivity solutions, which can be used to optimize the Cloud-Edge paradigm for cost-optimized use-case specific system solutions.

The innovation is a suitcase of adoptable solutions, and a practical demonstration on a currently unrealizable use case, namely an economically scalable digitalization of rail freight cars with wheel and bearing health sensors to reduce maintenance costs, reduce safety incidents, and increase productivity.

Component	Edge Sensors	**Partner**	NCG
Use Cases	Transport (PoC)		
Key Innovation	Neuromorphic context-based Data Clustering at the Edge as Data Science Enabler Situational energy optimized edge computing for Rail Health Determination Economically feasible Rail Heath Monitoring for Rail Freight Logistics		
Interfaces with	Highly Secure and Low-Power Compute Platform, Cellular IoT Connectivity		

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

3.2 Highly Secure and Low-Power Compute Platform

Sensors and actuators become IoT devices only by connecting them to a network, so that they can send measurements to control systems in a nearby MEC or remote data centre. To enable this cooperation, edge devices need local compute capacity to run communication protocols as well as cryptographic algorithms to protect control messages and data sent through the communication links. As a result, IoT devices run large amounts of complex software in order to meet all these functional requirements. This complexity is required for the device to fulfil its purpose, but it is also the enemy of security and reliability. As edge devices are critical for the trustworthiness of the IoT system as a whole, it is important that the on-device software is structured in such a way that security risks are minimized. Additionally, the security mechanisms provided by the underlying hardware are of critical importance to help the operating system (OS) protect device-specific software and state, all while minimizing the overhead for programs running on the system.

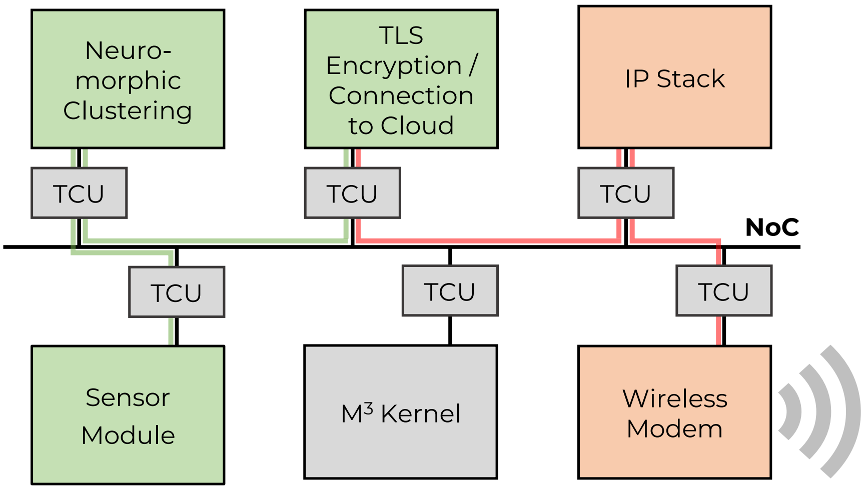


Figure 3.4: M^3-based platform with integrated neuromorphic sensor tiles and wireless modem

Barkhausen Institute (BI) contributes to the iNGENIOUS architecture a microkernel-based OS called M^3 and the tile-based computer architecture for which this OS has been designed. In contrast to commodity OSes such as Linux or real-time executives (RTOS), a microkernel-based OS is split into separate components that run isolated from each other. This construction principle makes a microkernel-based OS harder to attack, because a security vulnerability in one component will only compromise this one component, but not necessarily the entire OS. Additionally, M^3 applies the same isolation-by-default approach to hardware. To this end, it has been co-designed with the tile-based computer architecture shown in Figure 3.4. In this architecture, processing tiles are connected to a network on chip (NoC). Tiles do not access the NoC directly, but via a small hardware component called Trusted Communication Unit (TCU). The microkernel runs on one dedicated tile, while other components of the OS and applications are assigned their own, separate tiles.

The TCU is a data movement engine that enables message passing between tiles, as well as direct access to memory that is attached to another processing tile or a global DRAM (Dynamic Random Access Memory) tile. All these data transfers must be done via the TCU, as no other communication links exist in the hardware. The TCU will only allow communication between two tiles, if a communication channel to the target tile has been configured within the TCU. This configuration is done from the outside, via the NoC, by the microkernel running on its privileged processor tile. Other tiles lack the privilege to (re)configure any TCUs, including their own, so the microkernel is the only component in the system that can manage communication channels, while the TCU enforces the access-control policy efficiently in hardware.

Outsourcing access-control enforcement to the TCU has another advantage. It not only allows to integrate and police tiles with general-purpose processors (i.e., those that run software), but any other kind of hardware accelerator or I/O device can be connected to the NoC and managed in the same way. Simple sensors, specialized accelerators, or even complex I/O devices such as wireless modems can be integrated in an IoT device within a strict security regime.

Within the iNGENIOUS architecture, this capability is relevant in at least two cases:

1. Integration of the neuromorphic sensors, mandatory Transport Layer Security (TLS) encryption, and radio hardware employed in the transportation platform health-monitoring use case.
2. Efficient support of a flexible PHY/MAC, where signal processing may be offloaded in a secure way from baseband accelerators to general-purpose processing tiles.

In both cases, isolation of software and hardware components is enforced by the TCU, protecting confidentiality and integrity of data flows.

BI will also develop a minimal Root of Trust (RoT), which is integrated into the hardware, and corresponding OS support in M^3. The RoT is the basis of remote attestation and secure software updates in this platform.

Component	Highly Secure and Low-Power Compute Platform	**Partner**	BI
Use Cases	Transport (PoC)		
Key Innovation	Secure-by-default architecture Hardware root of trust		
Interfaces with	Edge Sensors, Cellular IoT Connectivity, Flexible PHY/MAC (UE Side), 5G Modem		

3.3 Immersive Devices

iNGENIOUS will use immersive devices for enhancing the health and safety conditions of workers in maritime ports and terminals. In particular, the project will explore the use of remote video telepresence, mixed-reality (MR) glasses and haptic devices for enabling the remote controlling of AGVs in real-time with human feedback. With these devices, operators will control the AGVs remotely in a safe mode, standing away from outdoors where hazardous working environments and adverse weather conditions can be encountered.

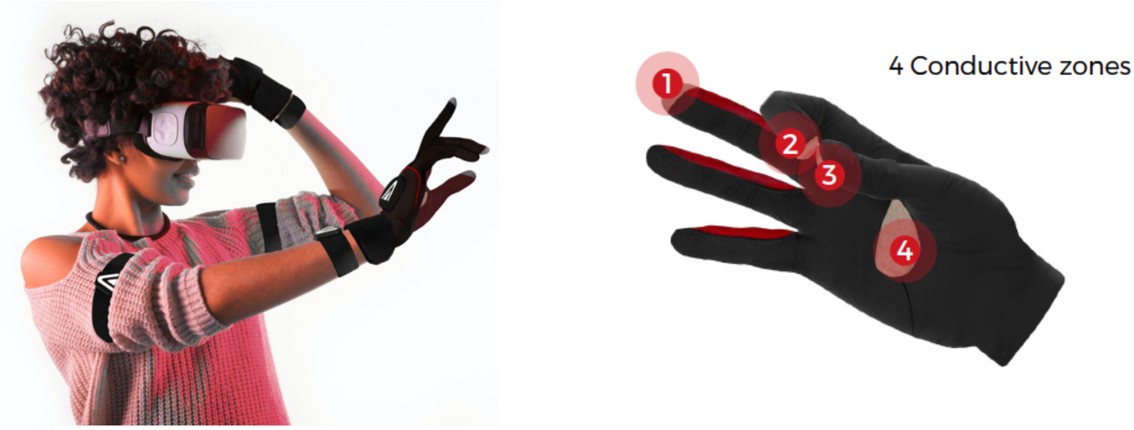


Figure 3.5: MR Glasses and Haptic Gloves

Mixed-reality glasses, which will be provided by NOKIA (NOK), will enable the enhancement of the driving experience while enabling the creation of a safer and more intuitive pilotage.

On the other hand, the interaction with the operator will be implemented with haptic gloves which allow to get real-time feedback remotely. Haptic gloves, which will be provided by Neurodigital (NED), consist of an array of 10 vibrotactile Linear Resonant Actuators (LRAs), Inertial Measurement Unit (IMU) based movement tracking, and gesture recognition capabilities. By including LRA components, gloves produce haptic feedback that will be used to provide warning signals to operators. Additionally, gloves include movement tracking capabilities by providing Full Finger Tracking enabled by 6 additional 9-axis IMUs (one per finger, except the thumb that has two). This technology permits to capture finger adduction, adduction and rotation degrees of freedom in contrast to Flex/Bending sensors which only provide one degree of freedom.

Complementing gloves, NED will explore the use of trackband accessories, which can be attached to the forearm and arm, and provide full upper-extremities movement tracking through direct kinematic algorithms. These trackbands work together with the glasses' own tracking system and provide a relative position with regard to the user's head position. Thanks to all these components, gloves are able to assess the user's physical and emotional suitability for task performance in working environments helping to identify posture, heart rate variability, and blood volume pulse, and to give information about fatigue, drowsiness, and stress.

Haptic gloves and glasses will be integrated into a remote-control cockpit, which will also include a steering wheel and pedals for controlling the AGV. For achieving an interaction between operators and AGVs, immersive devices will be complemented with the telepresence and sensing elements. Telepresence, which will be enabled by NOK, will be supported by four 120° low-latency video cameras and other proximity sensors installed in AGVs. These cameras and sensors will be used for the MR 3D visualization delivered to the cockpit's controller.

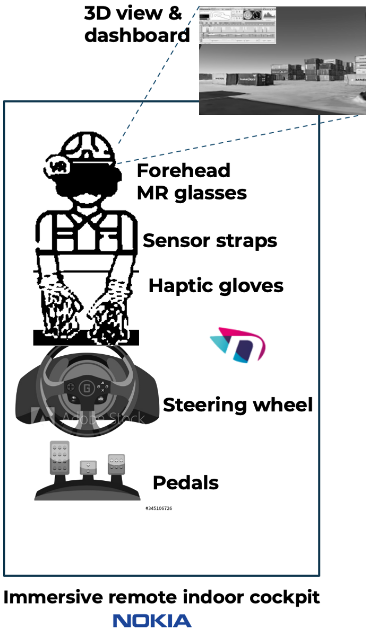


Figure 3.6: Immersive remote cockpit

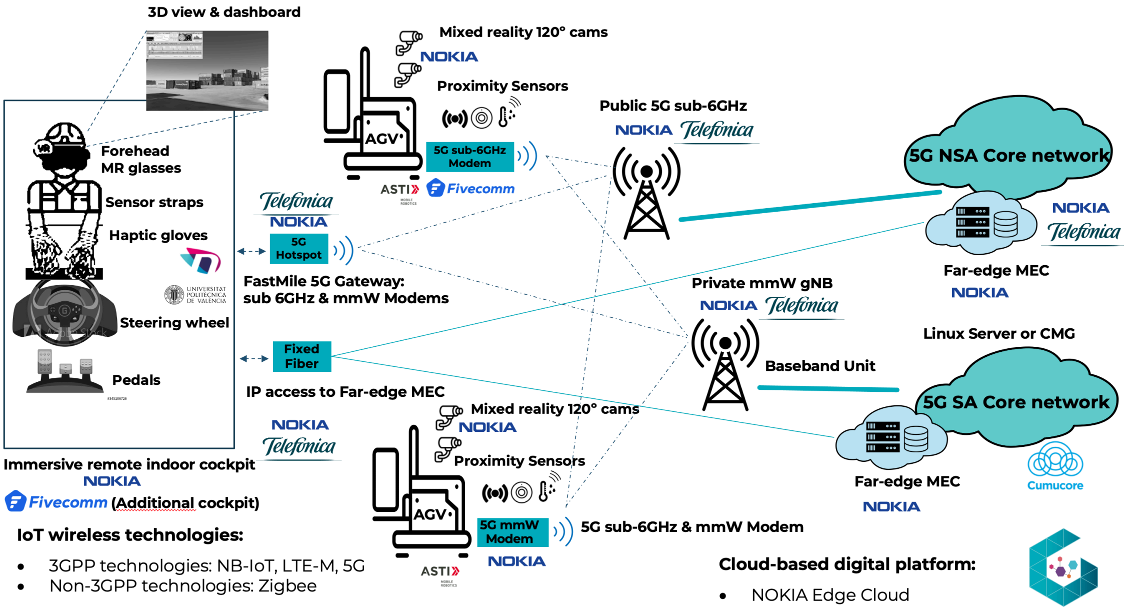


Figure 3.7: Overall architecture showing the immersive devices in the driver's safety use case

For enabling a secure and remote operation in dangerous working conditions, MR and haptic information flows will be transmitted in real-time conditions thanks to the use of 5G technology. In particular, all devices will be connected by means of 5G wireless modems and hotpots, which will be provided by Fivecomm (5CMM) and NOK to enable the achievement of stringent throughput (>100 Mbps), latency (≤ 10 ms), and reliability (≥ 99.999%) requirements. Thanks to 5G modems, the immersive remote indoor cockpit will be wirelessly

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

connected to an IoT 5G Radio Access Network (RAN) with corresponding data control services at a compatible far-edge MEC and related Core Network infrastructure. The interaction of all these components is shown in Figure 3.7.

Thanks to immersive devices, iNGENIOUS will improve the safety and work quality of machine operators in supply chain scenarios enabling: (i) enhanced safety of operational processes in dangerous working environments like port terminals or depots, (ii) very accurate operation with augmented vision or sensory data, and (iii) remote equipment maintenance operation.

Component	Immersive Devices	**Partner**	NOK, NED, 5CMM
Use Cases	AGV (demo)		
Key Innovation	Enhanced safety Remote equipment maintenance Increased accuracy of operational processes in maritime ports and terminals		
Interfaces with	Automated Guided Vehicles, 5G Modem		

3.4 Automated Guided Vehicles

iNGENIOUS will use automated guided vehicles (AGVs) for logistics transportation in maritime ports and terminals as illustrated in Figure 3.8.

When not operating autonomously, the AGV will be remote controlled in real time by using MR glasses and haptic devices. The AGV will receive commands remotely from operators who can take control of the AGV in hazardous working environments.

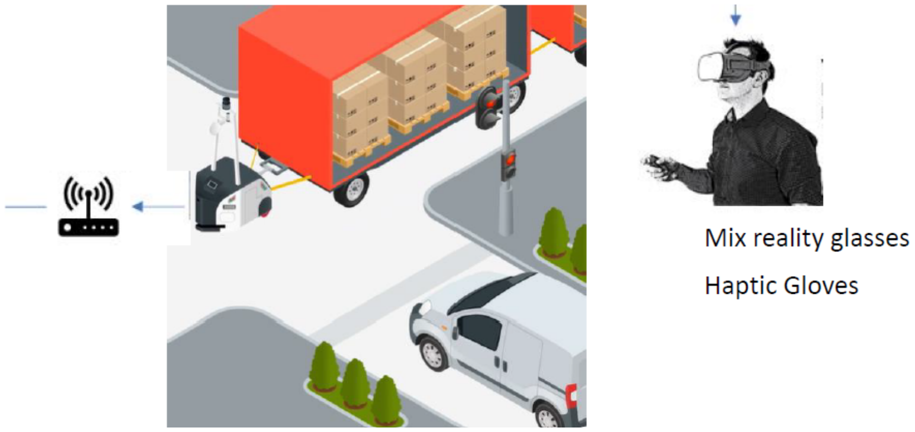


Figure 3.8: Remote control in hazardous environments

The remote control of AGVs will allow us to manage and solve unforeseen events (e.g., obstacles in the path, navigation issues, etc.) that can occur or maintenance operations, reduce reaction times, and avoiding interruptions in production or health and safety problems for workers.

Component	Automated Guided Vehicles	**Partner**	ASTI
Use Cases	AGV (demo)		
Key Innovation	Remote control of AGV with haptic gloves and MR glasses		
Interfaces with	Immersive Devices, 5G Modem		

3.5 Flexible PHY/MAC (UE Side)

The physical layer (PHY) is the lowest layer in a communications system. It connects the data source of upper communications layers to the physical medium. The medium access control (MAC) is used to control the access to shared media. In radio frequency (RF) communications, the MAC is responsible for allocating and scheduling the radio resources (time, frequency, and spatial). As illustrated in Figure 3.9, the PHY implementation can be split into:

- *Baseband module*, which is responsible for digital signal processing to encode/decode data to/from digital signals represented by in-phase and quadrature (IQ) samples. This module can be implemented with software or hardware depending on the performance requirements in terms of throughput and latency.
- *Radio front-end module*, which converts the digital signal at the transmitter (Tx) to an RF signal, and the received DF signal at the receiver (Rx) to a digital signal.

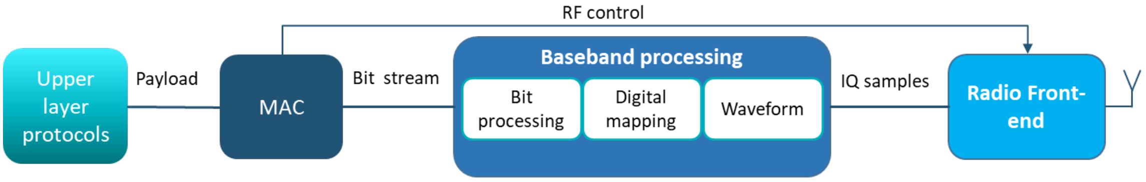


Figure 3.9: RF communications system architecture

In standards like 3GPP 4G and 5G, the baseband is split into three main modules:

1. *Bit processing*, which is responsible of performing bit level processing including scrambling, channel coding and interleaving
2. *Digital mapping*, which produces digital complex symbols by mapping several bits to one symbol, such using Quadrature Amplitude Modulation (QAM) mapping
3. *Waveform*, which generates the IQ sample using mostly linear transforms such as IDFT in Orthogonal Frequency Division Multiplex (OFDM)

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

The baseband at the receiver aims at decoding the information from the received discrete signal. The detection can be implemented in different ways and does not need to follow a specific standard. A common receiver design includes functions such as synchronization, channel estimation, equalization, and decoding.

Most of the RF communications standards employ a similar architecture. The differences lie in the operating carrier frequency and bandwidth, which can be controlled by means of a software-defined radio (SDR) RF frontend, in addition to the baseband and MAC techniques. Moreover, according to the OSI model, the communications layer 3 is mostly based on Internet Protocol (IP), and the standards define protocols in layer 2, which are implemented in software. PHY/MAC design following a defined standard is essential for commercial purposes. However, a device with fixed PHY/MAC implementation on a dedicated chip will only operate with the targeted standard. In contrast, a flexible implementation allows devices to be upgradable and reconfigurable to extend their lifetime. Moreover, the flexibility enables the development of private PHY/MAC in a private network, such as industrial networks. Finally, for research purposes, flexible PHY/MAC allows real-time experiments of new innovations in PHY/MAC design under realistic channel conditions instead of using simplified simulation.

The flexibility of the PHY refers to the ability to change the baseband parameters. The common baseband parameters are the code rate and the digital mapping order, which is known as modulation and coding scheme (MCS). In 5G New Radio (5G NR), further flexibility is added by controlling the IDFT (Inverse Discrete Fourier Transform) size. However, the channel coding and digital mapping functions are fixed to predefined implementations. A fully flexible solution is able to holistically change the overall baseband function. This allows to support non-OFDM based PHY and to create optimized functions based on given requirements, hardware constraints, and channel status.

The baseband hardware processing requirements depend mainly on the required data rate, the regularity of transmissions, and the latency constraints. For low data rate and occasional transmission, it is feasible to realize the PHY on a general-purpose central processor unit (CPU). For some other cases a digital signal processor (DSP) is sufficient, while in other situations, hardware implementation is unavoidable. The CPU or DSP in the former two variants could be part of the highly secure and low-power compute platform described in Section 3.2.

The flexible PHY/MAC can be considered as a framework that provides:

- *Compile-time flexibility* to enable the optimization of the baseband architecture by means of generic parameters that can be instantiated to optimize the design for a certain device capability
- *Run-time flexibility* to change some parameters on the fly depending on the channel

By using reconfigurable hardware such as a Field Programmable Gate Array (FPGA), both types of flexibility are beneficial to optimize the hardware

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

resource consumption at compile time, and to allow significant flexibility in run time by proper design of the architecture. A compromise between software and hardware implementation can be exploited with a kernel-based architecture, as the one presented in Figure 3.9.

Alongside the flexible PHY, a flexible MAC is required to convey control information about the used PHY configuration in the case of run-time flexibility, i.e., when parameter changes need to be applied on the fly. Moreover, a flexible MAC design should be considered to work with specific compile-time configurations (e.g., to realize a standard MAC with a standard PHY). A customized MAC design based on the use case is another option. For example, a simple MAC with deterministic resource allocation can be considered to connect few devices to an access point. This helps in avoiding the complexity and redundancy of standard MACs that are intended to support general use cases. The flexible PHY/MAC at the User Equipment (UE) side is supported by flexible PHY/MAC at the access point, as will be discussed in section 4.2.

Component	Flexible PHY/MAC (UE Side)	**Partner**	TUD
Use Cases	Factory (demo), Transport (PoC)		
Key Innovation	Flexible PHY/MAC based on hardware-software codesign Customized PHY/MAC for private networks		
Interfaces with	Highly Secure and Low-Power Compute Platform, Flexible PHY/MAC (RAN Side)		

3.6 Cellular IoT Connectivity

Cellular IoT (CIoT) technologies, driven by the 3GPP standardization body, provide a reliable and secure solution for ubiquitous connectivity of IoT devices. iNGENIOUS will investigate the evolution of CIoT technologies while at the same time leveraging the use of existing CIoT-based solutions to communicate, when deemed efficient, various types of data collected and generated by IoT devices.

Generally, compared to alternative non-cellular technologies, CIoT can deliver the following benefits:

- New IoT services do not require installation of a new connectivity infrastructure to provide communications in the area of the desired IoT service when already covered by a cellular network operator.
- Reliable and predictable service performance (inherent traits of cellular technologies) while not relying on uncertain availability/interference of unlicensed spectrum, thus, reaching wide coverage quicker and at lower cost from reuse of the existing network infrastructure.

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

- Long-term support (since based on global standards) and future proof (since part of cellular communication deployments with plans over decades) with continuous evolution, while keeping backward compatibility for legacy devices.

Enhancements of 3GPP to support machine type communications (MTC) for IoT have a long history since the LTE era. In iNGENIOUS deliverable *D3.1 Limitations and improvement axis for the communication of IoT devices* [4] we analyzed in depth those enhancements. CIoT technology includes the existing NB-IoT and LTE-M solutions and initial massive machine-type communication (mMTC) requirements were addressed as part of 3GPP Rel-13/Rel-14 technologies development targeting low-power wide area (LPWA) networks. Since then, the two cellular radio access technologies have been evolving in each new 3GPP Release for improved performance (e.g., higher throughput, lower power consumption) and to become part of the 5G family of technologies [5].

In addition to the LTE-based CIoT technologies addressing the massive, low profile IoT objects, NR opens the door to the so called critical or industrial IoT objects, for communication of higher data rate with much stricter requirements in terms of latency and reliability. To this end, 3GPP Rel-16 introduced enhancements for Industrial IoT support via NR. Currently, in 3GPP Rel-17, specification work on several items directly related to CIoT or targeting NR-based enhancements to support IoT scenarios is ongoing, including: "*Rel-17 enhancements for NB-IoT and LTE-MTC*" [6], "*NB-IoT/eMTC over NTN*" [7], "*enhanced Industrial IoT and URLLC support*" [8], and "*reduced capability NR devices*" targeting to enable devices of much lower cost from legacy NR devices [9] while Rel-18 is expected to further enhance those items.

In addition, iNGENIOUS plans to use CIoT-based solutions in order to provide real-time data received from sensors and device platforms for demonstration purposes. Integration of the CIoT device with sensors in an ideal case could be to have sensor modules as dedicated discrete components while the rest of the system may be integrated into a single circuit. For instance, it is more and more common nowadays to have a root of trust integrated into the cellular modem circuit with the notion of iUICC (Integrated Universal Integrated Circuit Card). Similarly, Transport Layer Security (TLS) and crypto accelerators are also embedded in modem circuits to support the 3GPP security basics. An FPGA could integrate the various blocks, where the host (i.e., sensor/platform) communicates with the Cat-M or Cat-NB modem through a Universal Asynchronous Receiver Transmitter (UART) interface using AT commands. The FPGA-based prototype of the highly-secure and low-power compute platform described in Section 3.2 is a candidate within the iNGENIOUS architecture.

Since it will not be possible to tape-out a chip during the iNGENIOUS lifetime, existing CIoT-based solutions will be used. Although 3GPP currently is specifying Rel-17 and scoping Rel-18, today's CIoT market solutions include mainly (if not only) Rel-13 and Rel-14 LTE-based Cat-M/Cat-NB devices (Rel-15 features are now shyly being adopted by the ecosystem). Such low-power communication modules/modems that can be attached to a cellular network (thus, using LTE-M/NB-IoT cellular technologies) will be part of transportation health-monitoring and multi-modal asset tracking (i.e, Transport and Ship) use cases in iNGENIOUS.

Component	Cellular IoT Connectivity	**Partner**	SEQ
Use Cases	Transport, Ship		
Key Innovation	Investigation of new innovative air interface solutions for CIoT communication modems in line with improvements discussed in the 3GPP standardization body		
Interfaces with	Edge Sensors, Highly Secure and Low-Power Compute Platform		

3.7 Non-cellular IoT Connectivity

Non-cellular IoT technologies are also considered to be leveraged in iNGENIOUS for scenarios requiring more flexible and simpler deployments in order to extend existing network coverage and address dedicated use cases. In previous studies *D3.1 Limitations and improvement axis for the communication of IoT devices* [4] and *D4.1 Multi-technologies network for IoT* [10], iNGENIOUS has considered and analysed a wide range of non-cellular IoT connectivity technologies (Zigbee, Bluetooth, LoRa, Sigfox or Sony Eltres) as potential solutions to address specific requirements such as the simplicity of the deployments, good coverage in harsh environments, etc. Based on this analysis, the project will apply some of the aforementioned technologies to demonstrate Transport and Ship use cases.

In the Transport use case, iNGENIOUS envisions (but will not demo) the use of LoRa connectivity between sensor gateways on the transportation platform and stationery LoRa nodes forming a mesh network in areas with otherwise poor or non-existent coverage. LoRa connectivity will also be used in the Ship use case to enable wireless communications between the container and the vessel while the container is aboard. In particular, the container will integrate a LoRA communication module (i.e., a Non-3GPP communication modem) to transmit the data measured and collected by the IoT sensors to the Smart IoT Gateway, which will be installed at the vessel bridge. Within iNGENIOUS architecture, container sensors and the non-3GPP communication modem will be integrated within the Things layer, while the Smart IoT Gateway will be part of the Network layer.

In this second use case, LoRa offers the possibility to perform a very simple and effective deployment aboard the ship by just installing two communication modules and antennas at both the container and the IoT Gateway. In these conditions, LoRa is able to provide good coverage and connectivity independently of the container location inside the vessel, both on deck and in the hold. These aspects are critical and make LoRa the best choice since other cellular-IoT deployments would be more complex, more expensive and would require more time for performing the installation of the equipment aboard the vessel.

Component	Non-Cellular IoT Connectivity	**Partner**	NCG, SES, FV
Use Cases	Transport, Ship		
Key Innovation	*No new functionality is developed by the iNGENIOUS partners, but the existing non-cellular IoT connectivity solutions are critical to support the project's use cases.*		
Interfaces with	IoT sensors in the Container, Smart IoT Gateway (Network Layer)		

3.8 5G Modem

The 5G New Radio (NR) module, or 5G modem, is a UE device that is used to connect specific vertical components, such as robots, sensors, cameras, or AGVs to the 5G network. The modem enables the components to communicate with the Next Generation NodeB (gNB) wirelessly, enabling the machines to speak 5G. Figure 3.10 shows a schematic of the 5G architecture in a simple way. As shown in the figure, the modems could be integrated within the end devices.

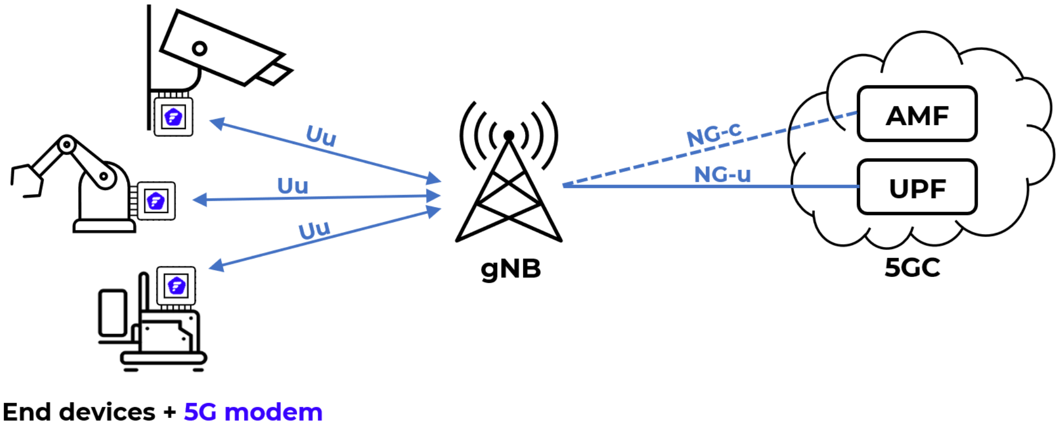


Figure 3.10: Contribution of the 5G modem in the system architecture

For an efficient implementation, 5G modems should be compact and integrated within the device, power efficient, simple, and usable as 'plug and play' devices.

Within the context of iNGENIOUS, 5G modems provided by Fivecomm (5CMM) will be integrated into the complete end-to-end system as part of the UE. These modems are both NSA (non-standalone) and SA (standalone) compatible. Note that an SA deployment here refers to the use of a single cellular technology, namely 5G, in both RAN and core parts, while NSA consists of the combination of 4G and 5G components in the same network.

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

The objective is to develop, integrate and validate a compact and flexible module solution that provides 5G wireless communication. The 5G modem is connected via Ethernet to the end device and connects to the 5G network via its integrated or external antennas. It is a powerful, versatile, and compact device designed to bring all the advantages of the new 5G technology.

The modem has simplified its electronics while minimising power consumption and cost. An overview of the 5G modem from Fivecomm is shown in Figure 3.11.

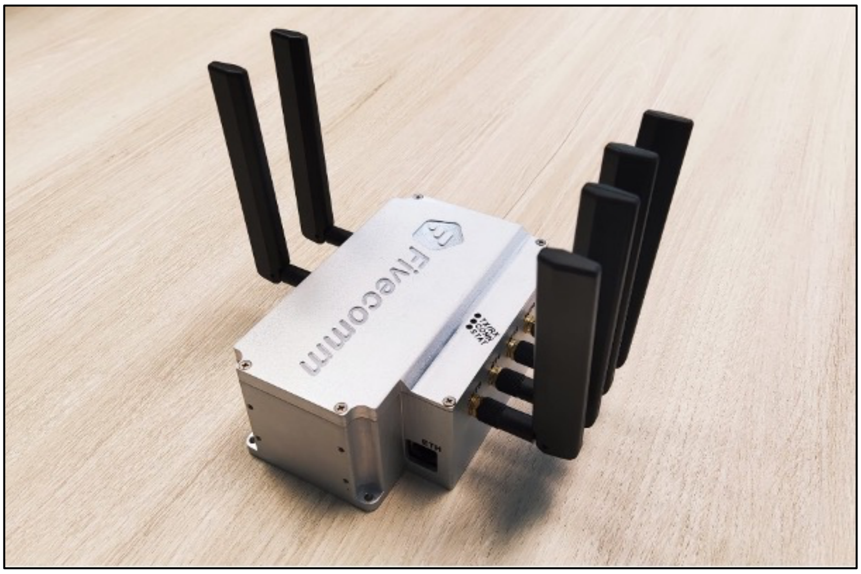


Figure 3.11: Fivecomm 5G modem (F5GM)

The 5G modem implements the following functionalities:

- *Easy deployment:* in a 'plug and play' fashion. It only needs to be connected to the power supply, use the Ethernet port to connect the end device, and fix the device to the infrastructure.
- *Customization:* Up to 6 antennas for providing the best experience even in low coverage scenarios. Ethernet or USB interfaces available.
- *Remote management:* It will include a management platform that allows to configure, monitor, and perform software updates remotely.

The modem supports the following technical features:

- *5G native mode:* both 5G NSA and 5G SA modes are supported, including options 3x, 3a and 2. 3G/4G connectivity is additionally supported.
- 5G NR Rel-15 support
- Sub-6 GHz frequency bands: n41, n28, n77, n78, n79, n40, among others
- Dual SIM
- Up to 2.5 Gbps in the downlink and 900 Mbps in the uplink

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

Component	5G Modem	**Partner**	5CMM
Use Cases	Factory (demo), AGV (demo)		
Key Innovation	Provides 5G wireless connectivity to any type of end device Easy to use (plug & play) Simple remote management for configuration, monitoring and software updates		
Interfaces with	5G New Radio (5G NR) End devices like Automated Guided Vehicles, Cameras, Robots (e.g., based on Highly Secure and Low-Power Compute Platform) connected via Ethernet interface		

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

4 IoT Network Layer

Networks consist of physical and logical components to interconnect different types of devices and computation platforms for the purpose of creating applications. The physical part of the network is responsible for the physical transmission of signals carrying data over media such as wires, optical fibres, and radio frequency (RF) channels. To allow multiple connections over shared channels, medium access control (MAC) and multiplexing schemes are used to coordinate the access to the shared medium in order to avoid interference and increase the utilization efficiency. The logical part of the network includes protocols and functions to enable communications over different types of physical media. On top of that, the network management governs the administration, operation, and provisioning of the network at different levels. The network can be split into access and core networks. The access part physically connects devices and gives them access to the network, whereas the core network connects different access networks and provides gateways to other networks.

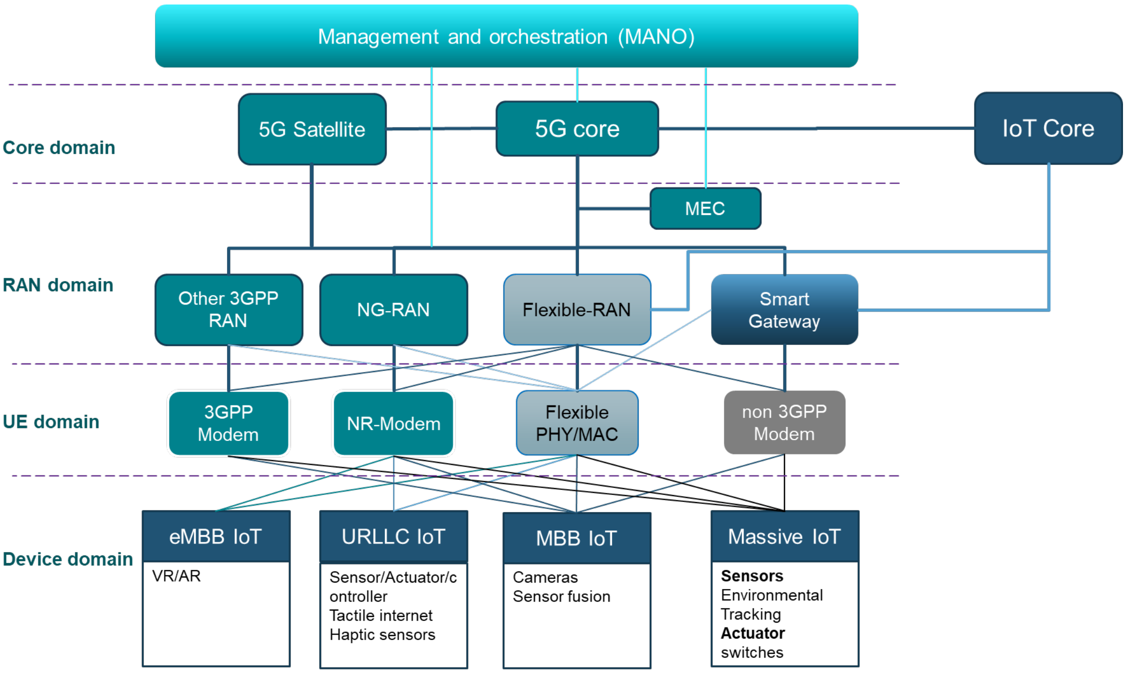


Figure 4.1: iNGENIOUS network architecture

Radio access technologies (RATs) are essential for providing connectivity, especially, for mobile devices and massive IoT. The existing wireless IoT solutions can be classified into 3GPP cellular IoT (CIoT) and non 3GPP IoT connectivity. The main purpose of IoT RATs was to provide best-effort connectivity to a massive number of low-complexity devices with battery constraints, such as sensors. These devices require very low data rates and relaxed latency constraints. They have been used to collect monitoring information. This type of IoT use case is referred to as Massive IoT. The emerging use cases in different business sectors demand more stringent QoS and different requirements in terms of

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

data rate, latency, and reliability. Broadband IoT is a group of devices such as cameras that requires much higher data rates and lower latencies than massive IoT. Industrial automation IoT use cases require small data rates but strict synchronization and reliability to allow integration with wired industrial networks. Other advanced use cases that employ mixed reality (MR) and tactile interaction with remote objects require high data rate and low latency. Different RATs have been developed to support a specific type of IoT. For instance, 3GPP provides massive IoT solutions based on 2G, 3G and 4G networks. Non-3GPP standards such as LoRa and Sigfox also focus on low power wide area (LPWA) access for massive IoT. On the other hand, WiFi has been extensively used to connect different types of IoT devices supporting broadband and massive IoT in a small range. Bluetooth has been used to connect a variety of devices, such as microphones, speakers, and wearables within a short range. Different wireless protocols for industrial networks have been developed based on IEEE 802.15.4 low-rate wireless personal area network (LR-WPAN) such as WirelessHART, Thread, ISA100.11 and ZigBee. The communication range is a factor of selecting the access technology. The cellular IoT initially considers wide coverage similar to other non 3GPP LPWA, unlike IEEE 802.15.4, IEEE 802.11, and Bluetooth, which all target short range. A hybrid solution is to provide long range connectivity by means of a gateway. This approach is used also to integrate different IoT devices in the cellular network without a need for dedicated cellular access functionality.

5G technologies aim at converging all types of IoT communication in one network. Thus, 5G will provide wide and local area access, and support the requirements of different use cases with one radio access network (RAN) and core infrastructure. Instead of developing independent network infrastructure for different IoT communication types, the 5G network will support that by means of network virtualization and slicing. In addition, 3GPP defines User Equipment (UE) categories for different IoT types to be supported in the same RAN and core networks.

The iNGENIOUS network interconnects heterogeneous access technologies to the 5G core network and the IoT core data network to support a wide range of available 3GPP and non-3GPP devices. While Chapter 3 introduced various devices, this chapter focuses on the RAN, core network, and management.

4.1 5G New Radio (5G NR)

The fifth generation of mobile cellular networks, 5G NR, has been designed to fulfill the requirements associated with three deployment scenarios: (i) enhanced mobile broadband (eMBB), (ii) ultra-reliable low latency communications (URLLC), and (iii) massive machine type communications (mMTC). eMBB is an evolution of the mobile broadband services that LTE offers, allowing for larger data volumes and enhanced user experience. URLLC is envisioned for services that require very low latency and extremely high reliability and mMTC corresponds to services characterized by a massive number of devices, for example remote actuators or sensors.

5G NR is therefore a fundamental pillar within iNGENIOUS use cases. But 5G NR is not the only technology that will be explored in the project. Other RAN technologies, which are currently being developed, will be considered. This includes O-RAN, which brings a more virtualized approach to RAN architecture. This implies a more flexible network, allowing for interoperable networks between different vendors, which share the same open-source software.

4.1.1 INGENIOUS RAN ARCHITECTURE

WP4 aims to provide a RAN architecture for the next generation of IoT devices. This RAN will be able to interconnect many nodes and give service to thousands of devices within a wide range of requirements such as data rate, latency, coverage, or mobility. The RAN will be connected to the 5G Core (5GC) through a standardized interface using fiber optic. This will allow all connected devices to be connected to the Internet.

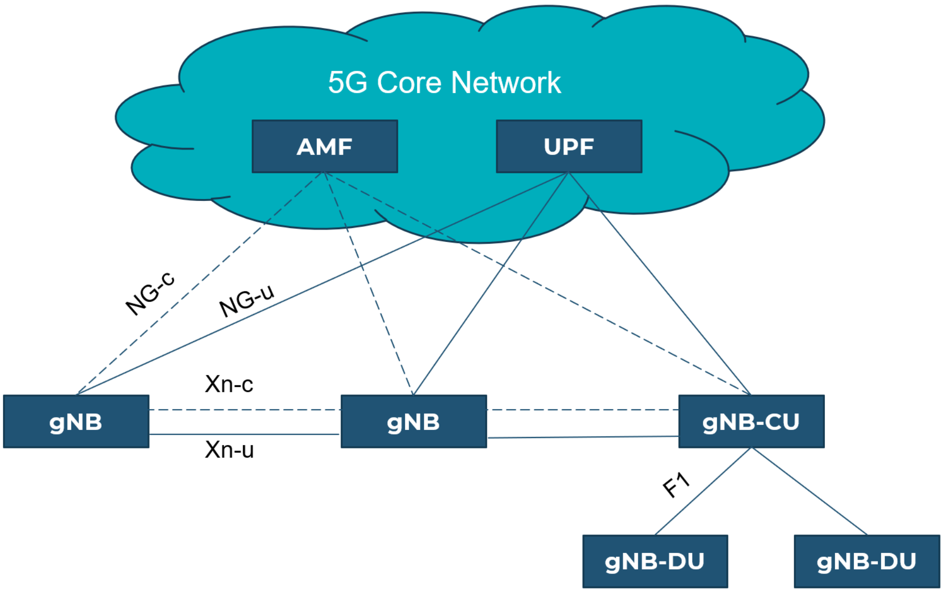


Figure 4.2: 5G Radio Access Network and interconnection with the 5GC through the AMF and UPF functions

The starting point of the iNGENIOUS RAN will be the 5G RAN, also known as NG-RAN. It consists of the combination of LTE eNBs (Evolved Node B) and NR gNBs (Next-Generation Node B) for radio access. In LTE and 5G NR, there is a Control/User Plane Separation (CUPS), which splits control and user plane functions. The control plane functions take care of the user connection management as well as user authentication, by defining some aspects such as the quality of service (QoS). User plane functions, on the other hand, deal with data traffic forwarding. This separation permits to scale user plane functions independently, driving operators to a more flexible deployment and dimensioning of the network. For instance, if data traffic increases, more user plane nodes can be added without affecting the control plane functions.

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

The gNB is responsible for all radio related functions, like connection establishment, resource management, admission control, or QoS flow management. The gNBs which conform the NG-RAN, are connected to the 5GC though the NG interface, more specifically to the User Plane Function (UPF) using the NG user-plane part (NG-u) and to the Access and Mobility Function (AMF) using the NG control-plane part (NG-c). gNBs can be interconnected via the Xn interface to support active-mode mobility, dual connectivity, Radio Resource Management (RRM), and lossless mobility between neighboring cells.

In turn, gNBs can be split in two parts: a central unit (gNB-CU) and one or more distributed units (gNB-DU) that are connected using the F1 interface. The Radio Resource Control (RRC), Packet Data Convergence Protocol (PDCP) and Service Data Adaptation Protocol (SDAP) protocols reside in the Central unit, and the Radio Link Control (RLC), Medium Access Control (MAC), and physical layer (PHY) in the Distributed unit.

4.1.2 SELF-OPTIMIZING RAN NETWORKS

iNGENIOUS will take NG-RAN as a basis and go a step forward. Partners will design an intelligent RAN, allowing for the management of the network to improve its capabilities. The introduction of intelligence and a more flexible architecture will allow operators to fully optimize their resources, as well as reducing operating expenditures (OPEX) and capital expenditures (CAPEX).

Self-Optimizing Networks (SON) were introduced in LTE to reduce the OPEX required to configure complex networks manually and to optimize performance, as described in 3GPP TS 36.300 [11]. These functions encompass solutions for network self-configuration, self-optimization, and self-healing. Self-configuration functions are the process where newly deployed nodes are configured by automatic installation procedures to get the basic configuration for system operation. These functions will also be applied in failure cases in combination with fast failure detection mechanisms to provide automatic failure recovery or compensation mechanisms [12]. On the other hand, LTE self-optimization functions are defined as the processes where Evolved Node B (eNB), UE, and Key Performance Indication (KPI) measurements are used to autotune the network [11]. Furthermore, self-healing functions encompass mechanisms for automatic localization and detection of failures, as well as techniques for healing the detected failures. This makes the network more resilient so that it can serve its customers even in case of unexpected events or changes that risk a degradation of network performance [13].

SON functions are expected to be crucial components of 5G networks, as described in [14]. One of the main reasons is that 5G networks have many more cells and are more complex than previous generations due to the usage of higher frequencies and the mm-wave range, where SON automation is even more important. 5G SON is expected to utilize network management data, including alarms, measurements, analytical KPIs, quality of experience (QoE), and provisioning data to analyze the network behaviour, status, and traffic pattern. It is based on time and locations to predict the potential issues and to plan a solution in advance to resolve the issues before happening.

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

O-RAN brings a more flexible and intelligent approach to the NG-RAN, introducing new elements that will allow for the deployment of SON functions. These new intelligent elements are the Non-Real Time RAN Intelligent Controller (NonRT-RIC) and the Real Time RAN Intelligent controller (NearRT-RIC). The NonRT-RIC supports intelligent RAN optimization by providing policy-based guidance, ML model management and enrichment information to the nearRT-RIC. On the other hand, the nearRT-RIC enables near real time control and optimization of the different nodes' functions and resources thanks to data collection and actions over the interface between the nearRT-RIC and the nodes, called E2 interface [15].

The nearRT-RIC can collect a wide variety of KPIs, like node measurements, load-related measurements, UE measurements, etc., and make predictions based on this data. The O-RAN architecture will be used in iNGENIOUS to test and deploy new ML models for different RAN functions, like resource allocation, load balancing, and handover.

Component	5G New Radio (5G NR)	**Partner**	5CMM, UPV
Use Cases	Factory, Port Entrance, AGV		
Key Innovation	Artificially intelligent Open RAN		
Interfaces with	5G Modem, 5G Core Network, MANO		

4.2 Flexible PHY/MAC (RAN Side)

In order to support diverse RATs, the RAN need to be able to support a variety of RF configurations as well as PHY/MAC. A simple approach is achieved by employing multiple dedicated software-defined radio (SDR) RF transceivers that can be tuned to a certain carrier frequency and bandwidth. The baseband processing hardware can be shared to process the IQ samples corresponding to each RAT PHY/MAC as shown in Figure 4.3. As discussed in Section 3.5, UEs can also be equipped with flexible MAC/PHY, which allow fully flexible customized RAN.

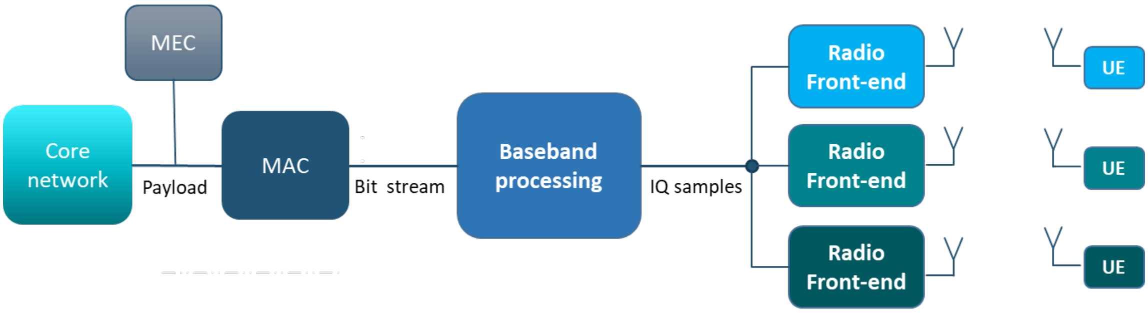


Figure 4.3: Flexible RAN architecture

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

In fact, this architecture supports different configurations in addition to multi-RAT. For instance, it can be reprogrammed to support multi connectivity or carrier aggregation. In addition, a private operator, especially in an industrial network, can employ a customized RAN with a privately optimized PHY/MAC per connected device. The RAN can then interconnect to the core network by implementing the required standard interfaces.

The flexible PHY/MAC allows to select the best configuration based on the channel status and application requirements. In 3GPP, the flexibility is limited to selecting the assigned resources, Modulation and Coding Scheme (MCS), the DFT (Discrete Fourier Transform) size, and precoding. A more general solution is to optimize the user signals by changing the encoding and waveform, and to flexibly provide multiple access schemes. The flexible MAC design includes conventional multiple access schemes such as Time-Division Multiple Access (TDMA), Frequency-Division Multiple Access (FDMA), Space-Division Multiple Access (SDMA), Code-Division Multiple Access (CDMA), and any combination of them. The flexible PHY/MAC approach contributes to the development of smart networking starting from the physical layer. The performance will be gradually enhanced by elaborating AI/ML data-driven techniques to assist the choice of different relevant parameters.

Component	Flexible PHY/MAC (RAN Side)	**Partner**	TUD
Use Cases	Factory (demo), Transport (PoC)		
Key Innovation	Smart flexible RAN transparently integrated to 5G core		
Interfaces with	5G Core Network		

4.3 5G Core Network

The ability to provide a big number of simultaneous connections interfacing the 5G Core and the MEC will lead to a design in which the core needs to be configured in a slicing mode that is more oriented to an mMTC type. It is also relevant to understand that some of the use cases will require a URLLC kind of slicing. So, on the one hand, the 5G Core–MEC interfaces might be tuned to achieve this, but a different architecture in the MEC part will require the existence of a big number of lightweight VNFs that will take care of the IoT communications and management. Open Source MANO (OSM) for the orchestration part and a customized Openstack/Microstack installation will handle the balance between the different types of services. A careful IP plan including the Virtual Local Area Network (VLAN) grouping of several levels and degrees of specialization will also be required (e.g., very low latency, few connections – low latency – reasonably high number of connections, etc.). These profiles can be prioritized and configured in an advanced optical switch between the core and the MEC which offers the possibility of tuning thresholds and capacities.

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

Far-edge components are understood as the set of processing devices which are capable of communication, management, and exchange of data with the cloud and the near-edge infrastructure. The project will not make use initially of Software-Defined Networking (SDN) capabilities in this layer although this is something that could be taken into consideration in the future. Typically, the idea is that this layer will be comprised of low/mid power consumption devices such as AI capable boards (e.g., Nvidia Jetson Xavier NX), which are capable of encoding video in real time and/or even execute some simple neural networks for object detections or simple predictions. In order to achieve security in this part, it would be interesting connecting them with the near edge using a Virtual Private Network (VPN) architecture. Other interesting activities that could be executed in these devices are anomaly detection, firmware upgrade management of IoT devices, and video streaming.

A classical Multi-access Edge Computing setup with reduced hardware specification compared to a full MEC installation may also be installed in a position which is closer to the IoT devices but farther away of the core in terms of laency. In case this option is deployed, it will integrate the same functionality as the near-edge MEC but installed in a lighter hardware specification.

Component	5G Core Network	**Partner**	NOK
Use Cases	Factory, AGV		
Key Innovation	Customized VLAN connectivity, User Datagram Protocol (UDP) Video Support, VPN capabilities		
Interfaces with	5G New Radio (5G NR), MANO		

4.4 4G/5G Packet Core

The 4G and 5G mobile packet core consists of multiple network functions that implement all the required functionality such as device authentication/authorization based on SIM information, handover across different radio base stations, and assignment of an IPv4 or IPv6 address to the device for connecting to a private or public fixed data network. The mobile packet core has been evolving from 2G to 5G where initially all the functionality of the mobile packet core was monolithic and tightly integrated with the hardware. In the latest specifications of the 4G/LTE, the mobile packet core named Evolved Packet Core (EPC) became modular and network functions were distributed as software elements on commodity hardware. Moreover, 5G continues in the modularity of the network functions towards micro-services and fully virtualized modules.

The iNGENIOUS use cases will utilize a 3GPP compliant Packet Core that includes 4G EPC and 5G Core (5GC), supporting both Non-Standalone (NSA) that integrates 4G and 5G together and Standalone (SA) functionality. The system can be deployed in bare metal or virtualized platforms (e.g., OpenStack,

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

Kubernetes) and provides a unique framework to build industrial and private networks. The design is focused on flexibility, cost reduction, and efficiency leveraging the advantages of Network Function Virtualization (NFV).

The 4G EPC consists of 3GPP Rel-15 compliant Mobility Management Entity (MME), Serving Gateway (S-GW) and Packet Data Network Gateway (P-GW) network nodes, and customized Home Subscriber Server (HSS). The 4G EPC also includes Narrowband IoT (NB-IoT) compliant with 3GPP Rel-13 and supports CIoT with a Service Capability Exposure Function (SCEF) module to deliver sensor data to application processing. In case of distributing a certain amount of data to large number of devices such as sensors, the EPC also includes enhanced Multimedia Broadcast Multicast Service (eMBMS) functions to multicast data to the end devices. eMBMS includes the standardized xMB interface defined in 3GPP Rel-16, allowing to establish a media broadcast service through an application programming interface (API). All the supported EPC modules and interfaces are included in Figure 4.4.

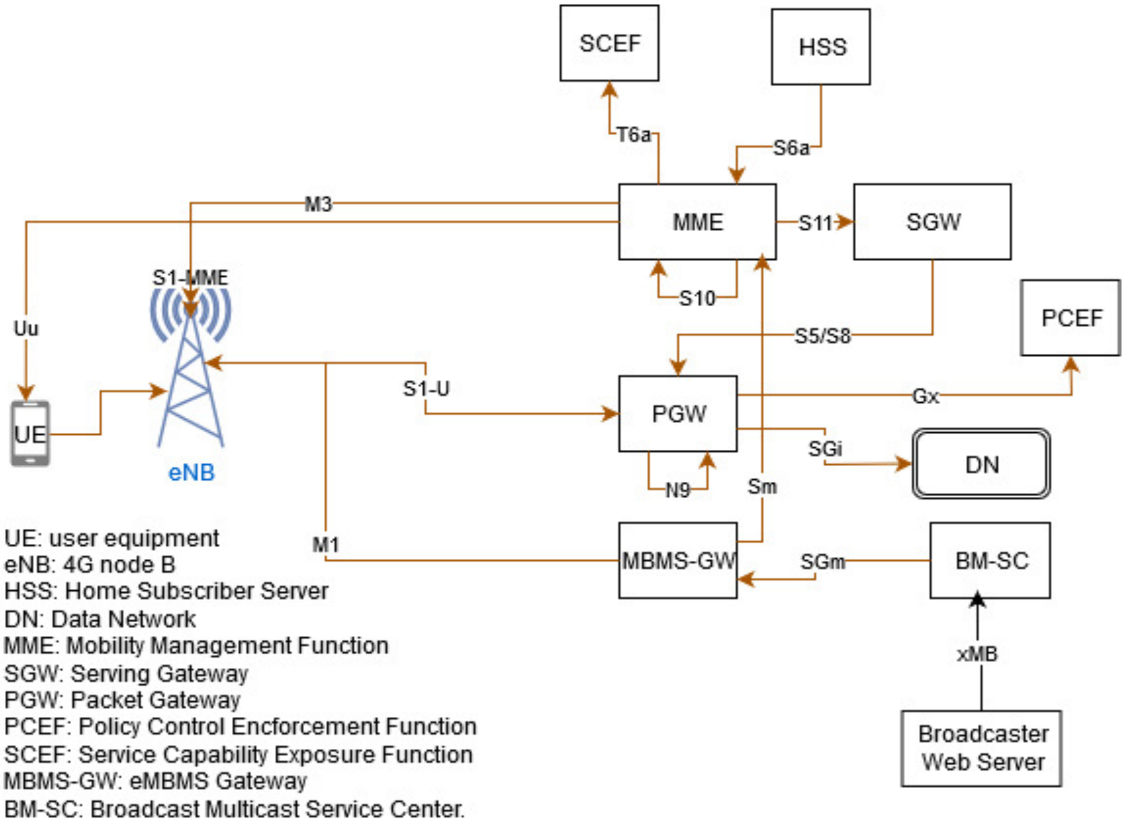


Figure 4.4: Modules of the 4G Evolved Packet Core (EPC)

The 5GC is 3GPP Rel-15 compliant and includes the modules depicted in Figure 4.5.

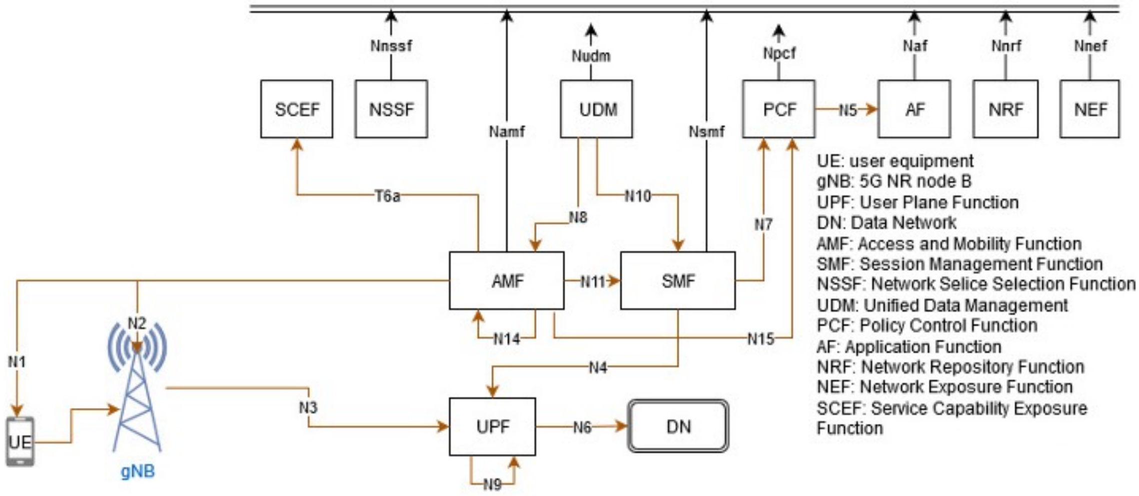

Nnssf
Nudm
Npcf
Naf
Nnrf
Nnef
SCEF
NSSF
UDM
PCF
N5
AF
NRF
NEF
Namf
Nsmf
T6a
N10
N8
N7
AMF
N11
SMF
N14
N15
N4
N1
N2
gNB
UE
N3
UPF
N6
DN
N9
UE: user equipment
gNB: 5G NR node B
UPF: User Plane Function
DN: Data Network
AMF: Access and Mobility Function
SMF: Session Management Function
NSSF: Network Selice Selection Function
UDM: Unified Data Management
PCF: Policy Control Function
AF: Application Function
NRF: Network Repository Function
NEF: Network Exposure Function
SCEF: Service Capability Exposure Function

Figure 4.5: Modules of Rel-15 compliant 5G Core (5GC)

5GC includes all the required functionality for interoperability with 3GPP Rel-16 and has been tested with different Radio Access Network (RAN) vendors. The current release of 5G Core (5GC) includes the network functions from Service Based Architecture (SBA) required for network slicing via Network Slice Selection Function (NSSF) and MEC discovery through the Network Repository Function (NRF).

Component	4G/5G Packet Core	**Partner**	CMC
Use Cases	Factory (demo), Transport, Port Entrance, AGV, Ship		
Key Innovation	Network Slice Manager Application Function (NSM-AF) that allows network operator to assign devices to different network slices		
Interfaces with	Session Management Function (SMF), Network Exposure Function (NEF), Unified Data Management (UDM), optionally NSSF and Policy Control Function (PCF)		

4.5 MANO

Supply chain scenarios like factories or maritime ports host thousands of objects and vehicles that need to intelligently cooperate with each other to carry out loading, unloading, handling, storing, and transport operations. Additionally, some elements like machinery, surveillance cameras, and access sensors need to be processed in real time with high reliability to enhance the operations and ensure the safety of the staff. To support different mMTC, URLLC, and eMBB use cases and satisfy the aforementioned system and user requirements, industrial scenarios need to deploy smart and secure network infrastructures able to dimension, split, and manage resources across different network slices while ensuring resource availability and high energy efficiency.

To be capable of orchestrating a heterogeneous set of use cases on top of a myriad of network technologies in different supply chain scenarios, iNGENIOUS will exploit a smart multi-tenant management and orchestration (MANO) layer. The iNGENIOUS MANO solution will be able to foresee the network requirements at both core and edge sides of the network infrastructure and ensure SLAs for covering different use cases in industrial scenarios like the Port of Valencia, Port of Livorno, or ASTI factory.

In practice, the iNGENIOUS MANO layer enables the management and orchestration of network slices in support of supply-chain and industrial use cases. The heterogeneous and at the same time strict requirements posed by supply chain and industrial IoT services in terms of network performance, time sensitiveness, reliability, and responsiveness can be satisfied by provisioning dedicated logical end-to-end networks. These logical networks are named network slices according to the 3GPP slicing principles and terminology and they span several network segments including RAN, edge, and core to interconnect different IoT devices and create seamless end-to-end communications. Network slicing builds on NFV principles defined by the European Telecommunications Standards Institute (ETSI) for the creation of isolated logical networks composed of IoT, RAN, edge, and core network functions in virtualized environments.

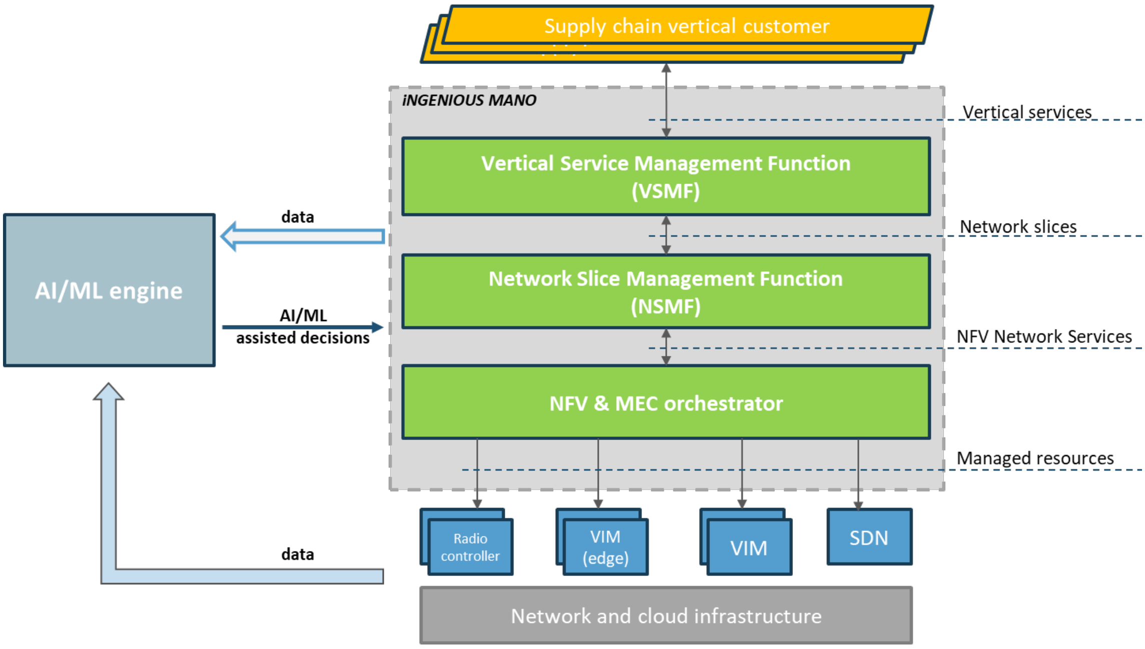


Figure 4.6: iNGENIOUS cross-layer network slice orchestration approach

To achieve this, the iNGENIOUS MANO is conceived as a cross-layer network slice orchestration framework with three main management functions that provide a complete integration of 5G NR, NG-IoT, and edge computing technologies as part of end-to-end network slices. This orchestration framework is shown in Figure 4.6. At the lower level, an NFV & MEC orchestrator interfaces with SDN network controllers for the radio and transport segments, as well as

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

with virtualized infrastructure managers (VIMs) at edge and core locations, to provision supply chain and industrial IoT services as NFV network services. On top of this first orchestration layer, a Network Slice Management Function (NSMF) takes care of the lifecycle management of end-to-end network slices, according to the 3GPP and GSMA slice orchestration principles and information models. As a vertical customer-facing orchestration layer, a Vertical Service Management Function (VSMF) is introduced to expose towards supply chain and industrial IoT verticals high level end-to-end services, called vertical services. The Vertical Service Management Function translates the custom vertical service constraints into network slices that need to be created in order to fulfil the specific supply chain or industrial IoT requirements.

As a key innovation, this iNGENIOUS cross-layer network slice orchestration framework tightly integrates with AI/ML functionalities to assist the operation and decision making of NG-IoT supply chain and industrial network slices, with the aim of optimizing them at runtime. This requires an AI/ML platform to consume heterogenous (monitoring) data from different sources, including the network slice orchestration layers themselves (each with specific resource, network slice, and vertical service-oriented performance-related information), as well as IoT and M2M data to be possibly retrieved from the iNGENIOUS Data Virtualization Layer.

Component	MANO	**Partner**	FV, NXW
Use Cases	Factory (demo), Transport, Port Entrance (demo), AGV, Ship, DVL/DLT (demo)		
Key Innovation	AI/ML assisted orchestration of NG-IoT network slices		
Interfaces with	5G Core Network, Data Virtualization Layer		

4.6 Smart IoT Gateway (Network Layer)

The Smart IoT Gateway (GW) is the system element responsible for the appropriate routing and sorting of sensor data, coming from one or more sensor networks to higher layer data consolidation services and M2M platforms. For performing these operations, the Smart IoT GW is able to interconnect multiple physical interfaces, as well as extracting and transforming messages as data traverses from one side to the other.

Taking the OSI model as a reference, the Smart IoT GW will expose several physical and data-link interfaces to receive sensor data. Sensors can send messages to the Smart IoT GW either wirelessly (with technologies such as IEEE 802.11, LoRa, or Sigfox), or directly connected to the device (via Ethernet, I^{2}C, or SPI) as shown in Figure 4.7. The Smart IoT GW will be smart enough to

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

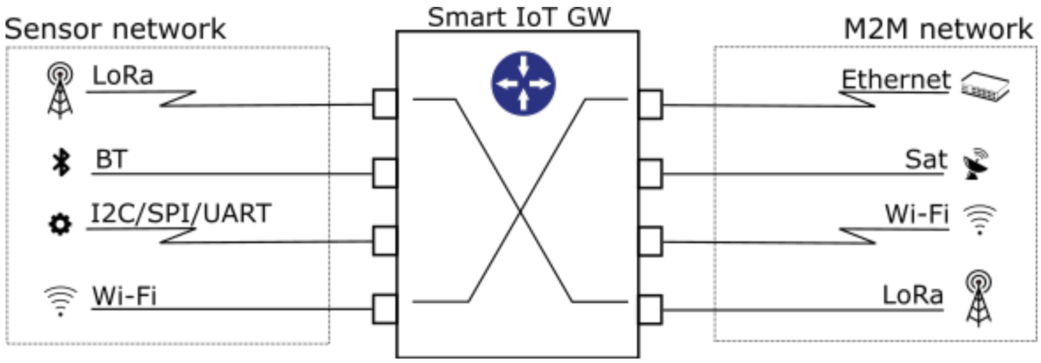


Figure 4.7: Smart IoT GW PHY interfacing

manage the routing and direct the received messages to the right output interface in the right timing. Several factors will be taken into consideration in this operation:

- *Context* such as the current geographical location of the Smart IoT GW or its situation relative to potential recipients of messages
- *Message prioritization* due to urgent messages that need to be forwarded immediately over other messages that can be grouped together for channel usage optimization
- *Channel availability* like in cases where constrained communications impose a specific interface linked to a channel, such as a satellite link when the Smart IoT GW is deployed on a ship sailing far away from the coast. In a diametrically opposed scenario, the ship would be moored in the port and the Smart IoT GW would favor a link established by 4G LTE taking advantage of a nearby mobile network station.

Physical interfaces are added to the Smart IoT GW as plug-in modules, that allow to abstract most of the device functionality from the number and type of the interfaces installed in the Smart IoT GW.

The Smart IoT GW also includes data-management functionality, which is discussed in Section 5.1.

Component	Smart IoT Gateway (Network Layer)	**Partner**	SES
Use Cases	Ship (demo), DVL/DLT		
Key Innovation	Support of different IoT protocols Message prioritization Detection, monitoring, and reporting on availability of backhaul connectivity Traffic optimized for satellite communications		
Interfaces with	Various connectivity options (LoRa, Bluetooth, I2C/SPI, Wi-Fi, Ethernet, MQTT over IP, HTTP(S), web sockets, Satellite Communications), 5G Core Network		

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

4.7 Satellite Communications

The satellite component of the iNGENIOUS architecture is part of the Network Core layer. The two options for satellite communication considered in iNGENIOUS are used as backhaul and through direct connection. Both are described in the following.

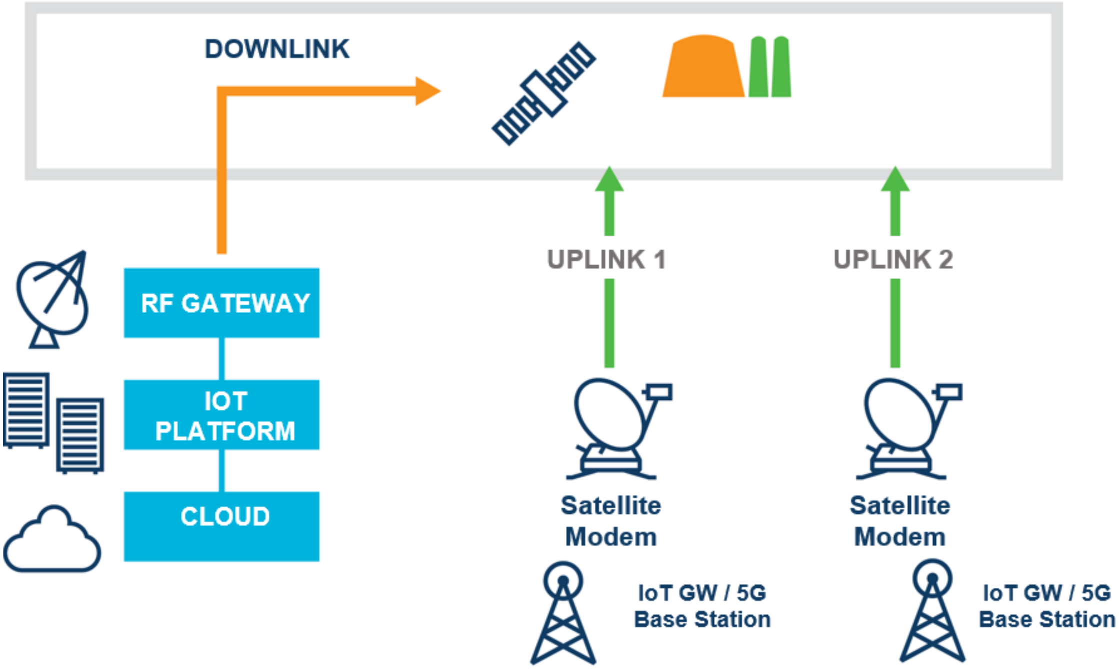


Figure 4.8: Satellite Backhaul

4.7.1 SATELLITE BACKHAUL

In collaboration with ST Engineering iDirect (iDR), SES will work on defining IoT backhaul systems, integration of core network to satellite and IoT, satellite and IoT edge computing.

Satellite backhaul serves indirect satellite access use cases, where the satellite network is used to backhaul and optimize the traffic from IoT devices. The purpose of satellite backhaul is to enable network operators to expand their reach into remote, rural and ultra-rural geolocations which are not economically served by terrestrial means, or that require a reliable backup to terrestrial backhaul. With this aim, network operators are able to meet the demands of their customers, providing 5G, IoT, and emergency services to all. ST Engineering iDirect's ground equipment is ideally placed to provide satellite backhaul solutions as they:

- Provide a standard IP interface to IoT Gateway equipment
- Have low CAPEX set-up costs

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

- Continuously lower operating expenditure (OPEX) costs due to technology features that:
    - increase throughput
    - improve spectral efficiency
    - utilize data compression techniques

Satellite backhaul not only serves the ubiquitous IoT demands of today, but is also well placed to serve the IoT demands of the future, as the backhaul density and throughput requirements expand. As part of this project, future satellite backhaul requirements will be explored, and new technologies researched and developed to improve and optimize the satellite backhaul use case.

4.7.2 SATELLITE DIRECT ACCESS

Unlike the satellite backhaul solution, direct access is where IoT devices are connected directly to the satellite network. ST Engineering iDirect plan to investigate the deployment of new and existing waveforms over satellite to support the direct access use case.

The investigation will include:

- An analysis of the current state of the art of Direct-To-Satellite IoT
- Considerations of the link budget requirements of a Direct-To-Satellite IoT solution
- A description of the components that are required to make up the solution
- Examination of radio technologies over satellite, including LoRa and CIoT (CIoT includes NB-IoT and LTE-M)
- New waveforms for IoT over satellite support
- The effect of the different satellite constellation types on a Direct-To-Satellite IoT solution

4.7.3 EDGE COMPUTING

In order to provide a flexible, scalable, and cost-effective means for satellite operators to deploy new services and provide an improved end-user experience, future satellite networks will have to be more closely integrated with their terrestrial counterparts. The continued convergence of telecommunication networks and information technology infrastructure, through approaches such as Software Defined Networking (SDN) and the use of Virtualized Network Functions (VNF) and MEC, is a key factor in ensuring satellite systems reach this objective.

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

Scenarios for integration of satellite components in future networks rely on softwarization/virtualization capabilities realized at the remote user site; either integrated within the satellite terminal itself or in a separate edge network node located closer to the data consumption (and production) of end users. Such edge network nodes will be capable of working with a variety of access schemes and device types, in line with MEC and the emerging edge network concepts being developed and applied in terrestrial networks. Such approaches can also help satellite to offer more effective solutions both from a performance perspective – some IoT services cannot tolerate the delay of a satellite backhaul link and local processing may therefore be a necessity – as well as from a cost perspective – not all data needs to be transported through a costly backhaul link as local processing can be done. Edge computing is even more beneficial to the end user in the satellite domain as the local edge processing has a greater impact on the latency experienced by the end user.

Component	Satellite Backhaul, Satellite Direct Access	**Partner**	iDR
Use Cases	Transport, Ship (demo)		
Key Innovation	Connectivity in areas where terrestrial networks cannot be used Investigation of direct satellite access in IoT devices		
Interfaces with	5G Core Network, Smart IoT Gateway (Network Layer)		

4.8 5G Security

Connected IoT devices and mobile applications require wireless network access that is resilient, secure, and able to protect individuals' privacy. The 5G system is designed with these requirements in mind. Thus, security and privacy play a critical role in 5G and parts of the iNGENIOUS architecture rely on the enforcement of these properties at the network level. Therefore, we summarize the key concepts of 5G security, although the project itself does not innovate in this area.

On top of the state-of-the-art encryption that is included in 5G, the trustworthiness of the 5G system is the result of five properties: resilience, communication security, identity management, privacy, and security assurance. From

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

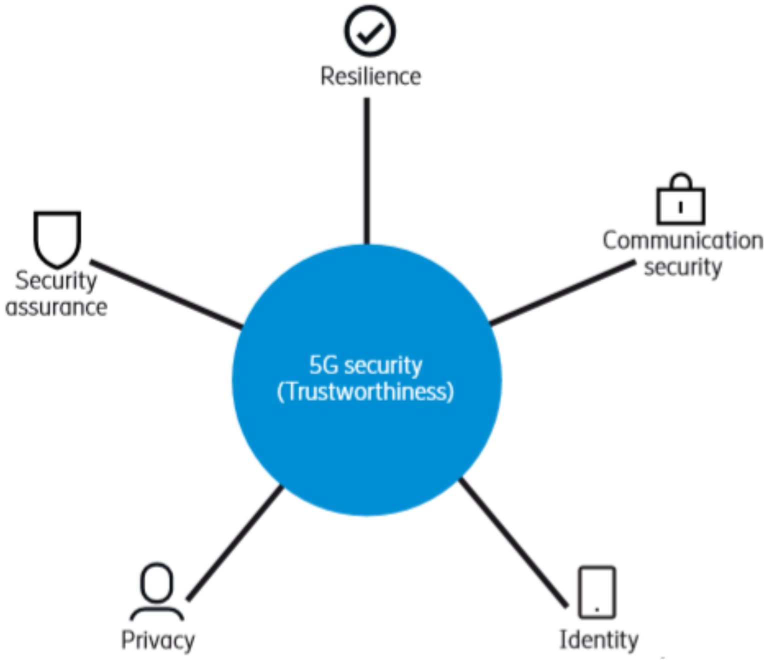


Figure 4.9: Properties for 5G trustworthiness

the 5G network point of view, trust in IoT is based on trustworthiness of the device's hardware, software, configuration, etc. Hence, trustworthiness is cumulative and will be defined by how well network operators and those who manage IoT devices govern the following:

- Identities and data
- Security and privacy
- Actor compliance with agreed security policies end-to-end

Interactions between user authentication, traffic encryption, mobility, overload situations, and network resilience aspects need to be considered together to build secure systems.

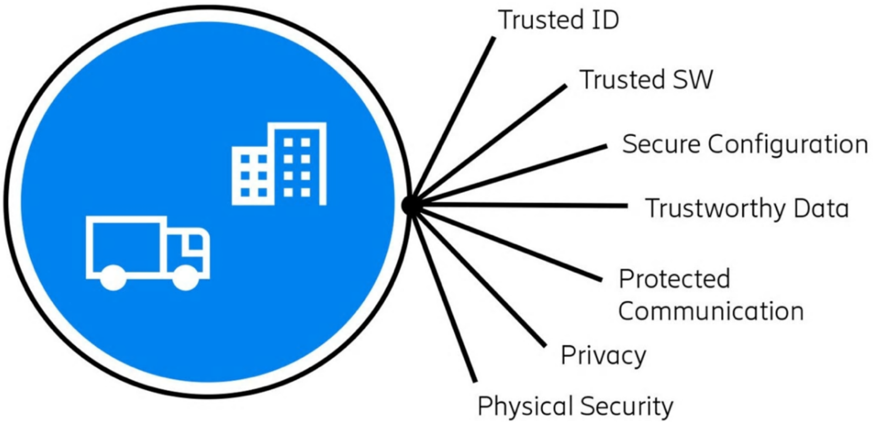


Figure 4.10: IoT device security aspects

The 5G core network architecture itself is designed around resilience concepts. Network slicing isolates groups of network functions from other functions. An operator may also isolate low-priority IoT devices on a separated slice to ensure that these will not interfere with other users. This isolation can avoid problems with large quantities of IoT devices. Network slicing enables the creation of device type, industry sector, or even customer specific subnetworks. The network slice control mechanism needs to provide appropriate slice management, configuration of access control, and secure isolation while still authorizing the shared resources. Each slice may have its own security policy that defines the security controls applicable for its specific threat landscape.

Software Based Architecture (SBA) principles are another architectural concept that enhances resilience. These principles make use of software and cloud-based technologies which has created a design shift allowing functions that can easily be scaled depending on traffic load, and can be independently replaced, restarted, or isolated when failing or under attack.

Overall, the 5G system provides secure communication for devices and for its own infrastructure. The 5G system includes protection against eavesdropping and modification attacks. Signaling traffic is encrypted and integrity protected. User plane traffic is encrypted and can be integrity protected.

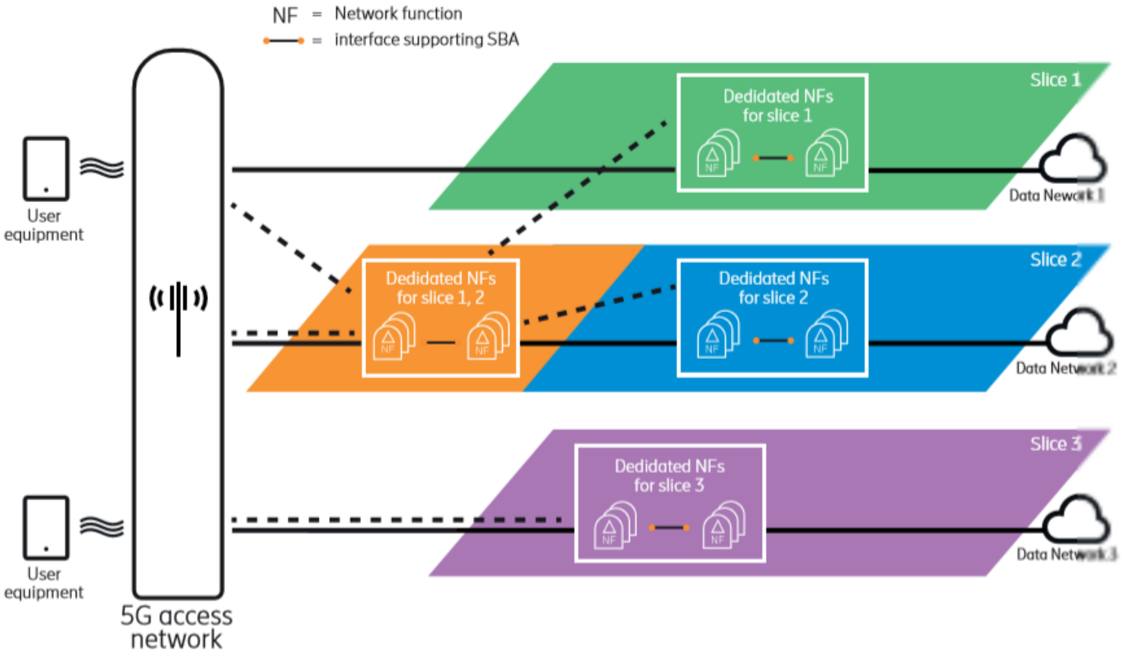


Figure 4.11: Network slicing in 5G

At its heart, the 5G system secures identity management for identifying and authenticating subscribers and devices, ensuring that only the allowed subscribers/devices can access network services. One of the most valuable new security features in the 5G system is the new authentication framework where

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

mobile operators can flexibly choose authentication credentials, identifier formats, and authentication methods for subscribers and IoT devices.

To address growing concerns and privacy legislation such as the GDPR, addressing the issue of privacy has been a high priority in the 5G system from the beginning so that subscribers' privacy is included by design. The devices and the network mutually authenticate each other and use integrity-protected signaling. This setup makes it infeasible for an unauthorized party to decrypt and read the information that is communicated over the air.

IoT is going to become one of the most important access domains for 5G, given the low-latency guarantees provided by the 5G system. IoT will feature a huge number of cheap devices of a wide technological variety. Such devices will offer a very big attack surface to malicious parties. Therefore, it will be of primary importance for 5G to contemplate anomaly detection mechanisms specifically targeted to IoT traffic. The highly secure and low-power compute platform described in Section 3.2 represents a possible solution to address the security challenge at the IoT device level. The underlying hardware/software co-design of this platform follows a secure-by-default approach, which makes devices harder to attack by design. Furthermore, it includes a hardware Root of Trust (RoT) that enables secure identification and run-time attestation of the integrity of the device. These properties and capabilities are a solid technological basis for being able to trust IoT devices. The platform could be integrated with the 5G security architecture in the future.

Another aspect of the 5G security that is investigated in iNGENIOUS is the policy analysis and definition for Identity & Access management for IoT devices.

Component	5G Security	**Partner**	N/A
Use Cases	Factory, Transport, Port Entrance, AGV, Ship, DVL/DLT		
Key Innovation	*No new security features are developed by the iNGENIOUS partners, but the existing 5G security features are critical to support the project's use cases.*		
Interfaces with	N/A (part of 5G Network)		

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

5 Data Management Layer

Nowadays, different parts of the supply chain like maritime ports, industrial factories, or logistics centres act as huge hubs of information due to the large number of processes that are carried out as part of the daily operations (e.g., arrival and departure of trucks, management and classification of stocks, storage of goods). Thanks to the digitalization of these industries, many of the information flows generated by processes have already been translated into large sets of data thanks to the use of M2M platforms, DLTs, etc. Nevertheless, supply chain ecosystems still struggle to process and manage large amounts of data due to the lack of interoperability between different systems, the use of analytics modules, and security and privacy mechanisms.

iNGENIOUS proposes an interoperability layer with data management capabilities that is able to ingest data from multiple sources by interoperating with different M2M platforms and DLTs, while ensuring security, immutability, and privacy aspects. Among other scenarios, this layer is a key component of the Ship (i.e, multi-modal asset-tracking) use case, where it collects data coming from IoT sensors that are installed on the shipping container.

At the lowest part of this layer, iNGENIOUS proposes the use of a Smart IoT GW able to collect and gather data from multiple IoT sensors and actuators by exploiting different types of IoT connectivity (e.g., cellular, non-cellular, satellite).

iNGENIOUS will exploit the use of different M2M platforms, which are used by different supply chain stakeholders for collecting and storing raw data in maritime, smart city, and cellular networks domains. On top of these data silos, the project envisages the implementation of a layer based on a Data Virtualization approach (Data Virtualization Layer, DVL), which will act as a federated and interoperable IoT layer for different M2M platforms and external data sources by providing shared access, management, and reading and writing capabilities to different entities (e.g., TrustOS, MANO and Awake.AI platforms, maritime events and truck-tracking dashboards) while ensuring security and privacy aspects following a role-based approach and applying pseudonymization techniques when needed (e.g., truck plate number). This cross-platform interoperability will enable the federation of different IoT platforms across heterogeneous domains, overcoming the compatibility issues between both standard and non-standard, proprietary, and custom M2M solutions widely used within the industry 4.0 verticals.

In order to provide secure and trusted data access to the end users, iNGENIOUS integrates a Cross-DLT layer on top of the DVL. By proposing a Cross-DLT layer, iNGENIOUS aims at creating a standard interface with a set of private and public Distributed Ledger Technology (DLT) networks (e.g., Bitcoin, Ethereum, IOTA, and Hyperledger Fabric). It serves as a single endpoint for interaction, orchestration, and management of different DLTs, including the storage of raw data (if supported by a given DLT), hashes and transaction histories.

Within the Cross-DLT layer, iNGENIOUS will also develop a decentralized identity mechanism for user identification as well as privacy and security technologies for data access protection.

The interoperability layer (based on DVL and Cross-DLT layer) is expected to be validated by means of a limited set of use cases within the project, namely the Port Entrance, Ship, and DVL/DLT use cases (i.e, *Situational Understanding and Predictive Models in Smart Logistics, Inter-Model Asset Tracking Via IoT and Satellite*, *Supply Chain Ecosystem Integration*). However, its potential goes beyond the selected application fields. From an architecture perspective, the interoperability layer can be also used in cross use-case scenarios, providing new data management capabilities for end users. The DVL suits fine for data lake management, regardless of the underlying physical layer, including physical devices and connectivity resources. For this reason, the DVL can act as a collector for data coming from different data sources and related to different application domains such as transportation, asset tracking, smart factories, and logistics.

Once data have been collected, processed, and aggregated by DVL according to supported data, the Cross-DLT layer ensures secure events management by means of different available DLTs. It allows end users to exploit native DLT capabilities for their own data (e.g., data existence proofs and data immutability). The following figure provides the high-level view of the interoperability layer in relation to considered use cases:

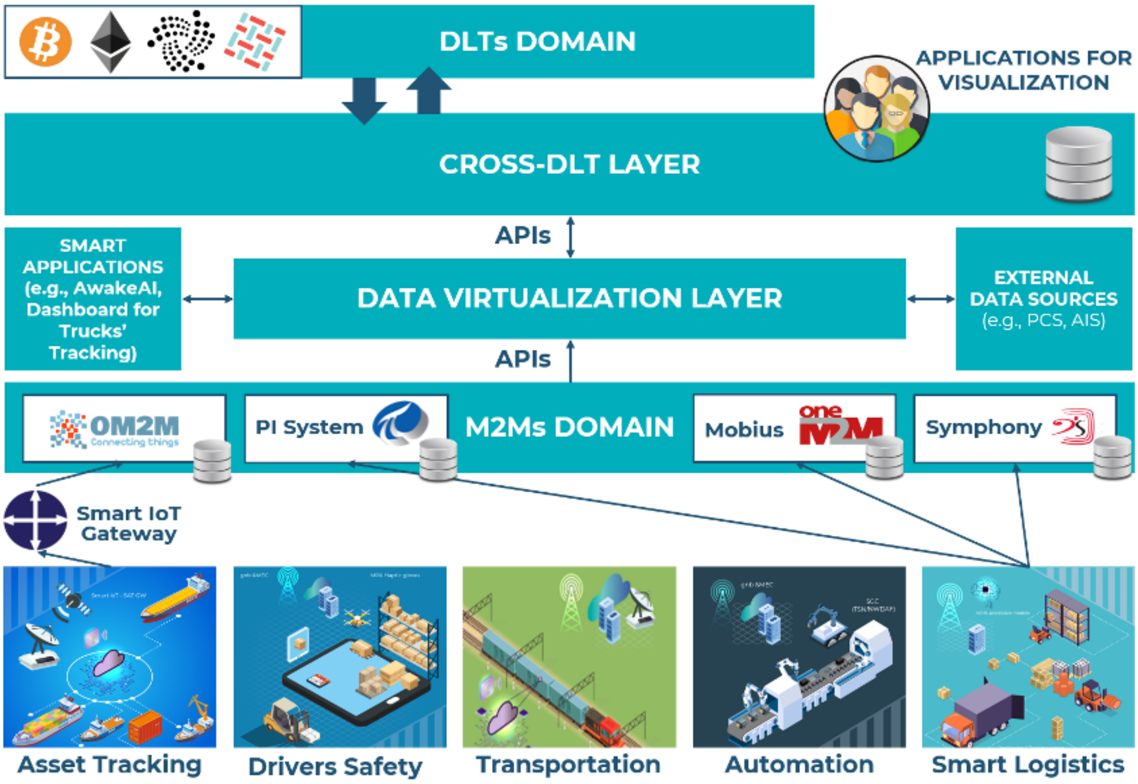


Figure 5.1: High-level view of the interoperability layer

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

The following sections describe the different components of the interoperability layer.

5.1 Smart IoT Gateway with Limited Data Management and Analytics Capabilities

The area of responsibility of the Smart IoT GW device spans upwards, from the network layer (see Section 4.6) into the data management and analytics layer of the iNGENIOUS architecture. In particular, the Smart IoT GW also provides configurable automated routing between connected parties, including message translation and local data management and limited analytics.

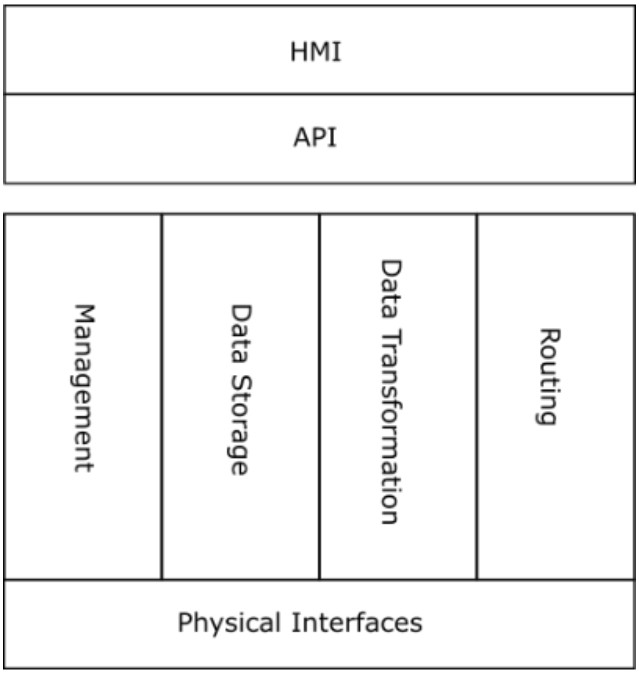


Figure 5.2: Smart IoT GW Data Management

The Smart IoT GW is composed of different logical building blocks to address the different data handling requirements as shown in Figure 5.2:

- *Sensor software interfaces*, which are responsible for receiving sensor data from connected sensor networks. These interfaces can also establish a bi-directional link with devices that support this type of communication
- *M2M software interfaces* that are exposed to M2M platforms that will receive and consolidate data processed by the Smart IoT GW with destination at the M2M platforms
- *Management endpoint* that provides local GUIs for management of the internal components
- *Local data storage* including limited-time expiring storage and standard persistent storage

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

- *Smart routing* that allows the interconnection of different endpoints
- *Data Transformation Service* which provides message translation

Internal metrics and configuration will be exposed by a local Application Programming Interface (API) that will allow external interoperability and system level automation.

Summarizing, the Smart IoT GW exposes external interfaces for M2M platform communication. The data transferred will be processed by the M2M wrappers and consumed by the DVL and upper layers in the Interoperability Layer.

As this communication will be over standardized interfaces, more specifically the oneM2M set of standards [16], the Smart IoT GW will implement the openMTC framework as part of its Data Transformation and Routing services. This eases the flow of data and simplifies the implementation on both sides of the interface.

Component	Smart IoT Gateway with Limited Data Management and Analytics Capabilities	**Partner**	SES
Use Cases	Ship (demo), DVL/DLT		
Key Innovation	Management endpoint Local data storage Smart routing Data transformation		
Interfaces with	M2M Platforms, IoT sensors		

5.2 M2M Platforms and External Data Sources

In this section, we describe a complete set of M2M platforms to be used within different use cases foreseen by the project as well as external data sources that will feed the Data Virtualization Layer. We also state how these components fit into the iNGENIOUS architecture according to considered use cases.

For the asset tracking use case, Eclipse OM2M platform is expected to be used for data retrieval and storage. The main data to be stored will come from the IoT devices and sensors installed on the container by collecting data related to its status such as: location of the container, temperature, humidity, vibration, bump detection and door opening (or seal removal).

Mobius OneM2M, PI System OSIsoft and Symphony platforms are part both of smart logistics and supply chain ecosystem use cases and will be used at Port of Livorno and Port of Valencia accordingly. As far as the Port of Livorno is concerned, Mobius OneM2M platform will provide historical meteorological data sets that will be extracted by DVL and then consumed by Awake.AI platform for predictive analysis. Gate-in and gate-out data will be retrieved from the port community system instead (Tuscan Port Community System - TPCS). It is also planned to use Symphony M2M at the Port of Livorno in order to collect and expose to the DVL data coming from tracking device installed on operative vehicles (with the aim of simulating trucks running within the seaport area). PI System OSIsoft will be used as M2M platform at the Port of Valencia in order to store and then make available data related to gates' access. In this testbed, AIS data source is not going to interact with Data Virtualization Layer: vessels positioning data will be directly ingested into Awake.AI platform in order to find out any correlation with the truck turnaround time (TTT). Moreover, data related to port calls will be directly extracted from the ValenciaPCS (port community system) and consumed by Awake.AI platform by means of an API.

The Data Virtualization Layer (described in the following section) will act as a data aggregator between the above-mentioned data sources according to maritime events data model, so that the Cross-DLT (Section 5.5) layer can securely distribute them over different DLTs by storing the associated hash.

Component	M2M Platforms and External Data Sources	**Partner**	CNIT, SES, NXW, FV, AWAKE, AdSPMTS
Use Cases	Transport, Port Entrance, Ship, DVL/DLT		
Key Innovation	*M2M platforms as well as external data sources are part of the overall architecture, but no relevant innovation is expected here. Instead, iNGENIOUS partners rely on the current state-of-the-art of such technologies.*		
Interfaces with	Data Virtualization Layer, Awake.AI Platform		

5.3 Data Virtualization Layer

Data Virtualization can be considered as a responsive data integration/aggregation approach that allows its consumers to connect to multiple data sources, extract defined data and create a single view of them by providing aggregated information. This simplifies information access for big data, analytics, business intelligence, and data lake access purposes. On the other hand, the Data Virtualization approach allows applications to retrieve and process these data without requiring technical details about the data in itself, such as how it is formatted or where it is physically located. In the iNGENIOUS project, we use the Data Virtualization Layer (DVL) as an intermediate layer to communicate with different data sources.

In the context of the supply-chain ecosystem-integration use case, data sources will be represented by different heterogeneous M2M platforms deployed in a maritime context as well as by different external data sources (e.g., port community system and automatic identification system). According to this, the DVL will be used for raw data collection and aggregation. The

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

aggregation process will be performed according to a given data model based on events such as gate-in, gate-out, vessel arrival, and vessel departure and eventually seal removal. Different M2M platforms will be available for their deployment in seaports such as Livorno and Valencia both during implementation and validation phases of the use cases.

The main platforms that will be considered are made available by the consortium and are listed below:

- Mobius OneM2M (CNIT)
- Symphony (NXW)
- PI System OSIsoft (FV)
- Eclipse OM2M (SES)

The above mentioned M2M platforms are operating in different contexts and during the development phase they will be instantiated within the maritime domain for the PoC validation (Port of Livorno, Port of Valencia, and COSCO ship). From a technical point of view, the following aspects have been considered during the M2M state of the art assessment in order to define development activities with regard to the DVL:

- Communication protocols: MQTT[1], CoAP[2], HTTP[3], MQTT-SN, CORBA[4], REST[5] API, gRPC[6] API, proprietary socket-based API, OPC UA[7]
- *Storage method:* non-relational and NoSQL databases (e.g., ElasticSearch, MongoDB), time series databases (e.g., influxDB), relational databses (e.g., PostgreSQL)
- *Frequency of incoming messages and bandwidth:* depends on considered events and the physical devices connected
- *Data Format:* RDF/OWL[8], JSON[9], UA binary, XML[10]

[1] MQ Telemetry Transport

[2] Constrained Application Protocol

[3] Hypertext Transfer Protocol

[4] Common Object Request Broker Architecture

[5] Representational State Transfer

[6] gRPC Remote Procedure Calls

[7] Open Platform Communications Unified Architecture

[8] Resource Description Framework, Web Onthology Language

[9] Javascript Object Notation

[10] Extensible Markup Language

As far as the Port Entrance use case on situational understanding in smart logistics is concerned, the DVL will be used for the interaction with (i) M2M platforms from Valencia and Livorno Ports (PI System OSIsoft, Mobius OneM2M, and Symphony), (ii) MANO platform for historical data analysis to assist its network and slice optimization logics, and (iii) the Port Community System from the Livorno Port (TPCS). These data will be then used to produce maritime events such as gate-in, gate-out, vessel arrival, vessel departure, and seal removal (part of the Ship use case on asset tracking). They will be used at DVL level, providing a virtual view for the Port of Livorno and the Port of Valencia, as depicted in Figure 5.1 on page 50. By means of this approach, the supply chain ecosystem use case will be also validated.

During the project lifetime, we will consider the possibility to run different synchronized instances of DVL in parallel in order to avoid a single point of failure.

Moreover, in order to be compliant with GDPR regulation, a pseudonymization function running at DVL level will allow to detect and obfuscate personal data (e.g., trucks' plate number or eventually truck driver registry) according to the techniques suggested by the European Union Agency for Cybersecurity (ENISA). It ensures that data subjects are hidden from any third party that is not allowed to gather such information. Only authorized entities will be able to re-identify pseudonymized data subjects.

Component	Data Virtualization Layer	**Partner**	CNIT, TEI, FV, NXW, SES
Use Cases	Transport, Port Entrance (demo), Ship (demo), DVL/DLT		
Key Innovation	Data virtualization Data federation Single access point for M2M platforms Personal data pseudonymization		
Interfaces with	Cross-DLT Interoperability, AI-based module of MANO, AI/ML Data Analytics from Awake.AI, M2M Platforms and External Data Sources		

5.4 DLT Solutions

Distributed ledger technology (DLT) promises to deliver an immutable ledger of transactions. This feature allows for strong proof that the data existed prior to a given point in time, namely when the data was stored on the ledger. Combining digital signatures with the hashes of the actual data, we can show that someone has recorded the data related to this hash. This information cannot be removed or modified, as explained in detail in iNGENIOUS deliverable *D5.1 Key technologies for IoT data management benchmark* [2]. iNGENIOUS combines different DLTs in order to give access to different levels of security and

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

performance. The DLTs were selected carefully to provide the widest spectrum of features. Bitcoin is the most stable and secure, but the slowest in terms of on-chain operation. It is designed to be “digital gold”, so features are added only after very careful testing, resulting in uninterrupted operation since 2013. Ethereum provides faster transactions on-chain and more complex smart contracts. IOTA is the fastest one in terms of transaction confirmation and is focused on IoT platforms, but it requires a central coordinator in order to maintain integrity of the Tangle. Both Ethereum and IOTA are in active development focused on providing new features, so they experience downtimes from time to time. Hyperledger is fast and scalable on-chain, but it is a private blockchain, so the external entities must trust owners of the ledger that the information is legitimate.

DLT usage is part of the overall supply chain ecosystem use case, based on data coming from asset tracking and smart logistics use cases, allowing its validation. In order to demonstrate the interoperability among different distributed ledger solutions, the iNGENIOUS consortium provides the following technologies:

- Bitcoin (deployed in PJATK facilities).
- Ethereum (deployed in Telefonica facilities).
- Hyperledger Fabric (deployed in FV and Telefonica facilities).
- IOTA (deployed in CNIT facilities).

The DVL will aggregate data coming from different data sources in order to make sure that maritime events are properly defined in terms of attributes: gate-in, gate-out, vessel arrival, vessel departure and seal removal. These data are defined according to data model adopted by another DLT solution called Tradelens, which clearly specifies what kind of parameters are requested. In order to achieve this, DVL needs to interact with several data sources in order to aggregate data and make them available in the form of a virtual view. Once data aggregation is performed it can be made available to Telefonica’s TrustOS, which is a framework and abstraction layer for building DLT-based applications. TrustOS has access to the specific view from DVL by invoking an interface (REST API) and can retrieve data of interest. At this stage, retrieved data are considered as raw data by TrustOS which stores them and creates a digital asset for their representation (TrusOS’ track module is expected to be used). Each digital asset will be also characterized by its own hash as well as by a full set of additional parameters (e.g., assetID, metadata, owner, data of creation, trust point, hash of the asset, etc.). After this first interaction, a trust point is created so that the proof-of-integrity can be guaranteed by distributing and storing it in different networks of different DLTs.

It is important to highlight that each available DLT has its own internal mechanisms for transactions, payments and/or wallets management and these details are left to DLT itself. We are focused on the interoperability aspects by means of TrustOS solution, which is described in the following section.

Component	DLT Solutions	**Partner**	PJATK, CNIT, TID, FV
Use Cases	Port Entrance, Ship, DVL/DLT		
Key Innovation	*DLT solutions are part of the overall architecture, but no innovation is expected in the project for this technology, as they are state-of-the-art. However, the project uses them to store TrustPoints in order to guarantee the proof-of-integrity.*		
Interfaces with	Cross-DLT Interoperability layer based on TrustOS solution		

5.5 Cross-DLT Interoperability

The Cross-DLT layer is conceived as a standard interface for enabling secure and trusted communications between DLT networks and M2M platforms through its connection with the DVL. Cross-DLT aims at enabling the interaction, orchestration, and management of smart contracts, as well as the storage of raw data, hashes, and transaction histories performed between different M2M platforms. The DLTs in the iNGENIOUS project are very diverse, so there is a subset of functionalities that are present in every DLT solution. The Cross-DLT layer is based on TrustOS by Telefonica. It provides storage capabilities for data arriving from the DVL and the timestamping methods that allows for data integrity verification. The data itself cannot be stored on every DLT mentioned in the project, so it will be stored in a database managed in TrustOS. A proof of data existence will be stored in the different DLTs for future integrity verification.

The most useful feature of the DLTs in context of the iNGENIOUS project is the immutability. This immutability of the stored data gives new possibilities in terms of timestamping. Traditional timestamps are recorded in a secure way by the trusted party (or internally in the organization). Employing immutable ledgers to store timestamps gives another level of trust. This trust appears because even if the entity responsible for storing the timestamps is compromised, it is still possible to verify the timestamp independently, using data on the DLT. Right now, there are already many ways to utilize DLTs for timestamping, because the idea appeared very early in the Bitcoin community (and later in the broader range of DTLs/blockchains). One possible way to proceed is to store the data itself on the blockchain. A better way is to store the hash of the data directly on the blockchain/DLT. Currently, because storing data on public blockchains is expensive in terms of transaction fees, time, and energy, the most widely used method is to organize hashes of data in the hash trees and recording the root of the tree on DLT. The inclusion proof can be independently verified by anyone who has access to the specific DLT. The example of this method is OpenTimestamp created in 2016 [17]. In iNGENIOUS we will implement similar mechanisms, but for a larger range of DLTs with a

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

common API, and also provide a common proof format that will allow for independent verification of the timestamp using direct interaction with specific DLTs. This way it will be possible to remove the need for trusting different entities that the data was not tampered, and instead assume that the data recorded on the DLT is immutable.

There are many different DLTs available, with different trade-offs. In iNGENIOUS, Bitcoin, Ethereum, Hyperledger, and IOTA will be used. Each of the DLTs has different design goals and therefore different features. Some of them are public (like Bitcoin, Ethereum), some are designed to be permissioned (Hyperledger, Tradelens), and there is IOTA that is mixture of both. There are also different main purposes. Bitcoin is for digital version of cash or gold that is designed to be verifiable and useable by anyone with even low-end computers, whereas Ethereum is designed as a platform for smart contracts and "world computer" with its innovative virtual machine and solidity language. IOTA is designed as low power DLT solution for the Internet of Things, Hyperledger (with Tradelens) is designed as a solution for a corporate blockchain with smart contract capabilities and permissioned access.

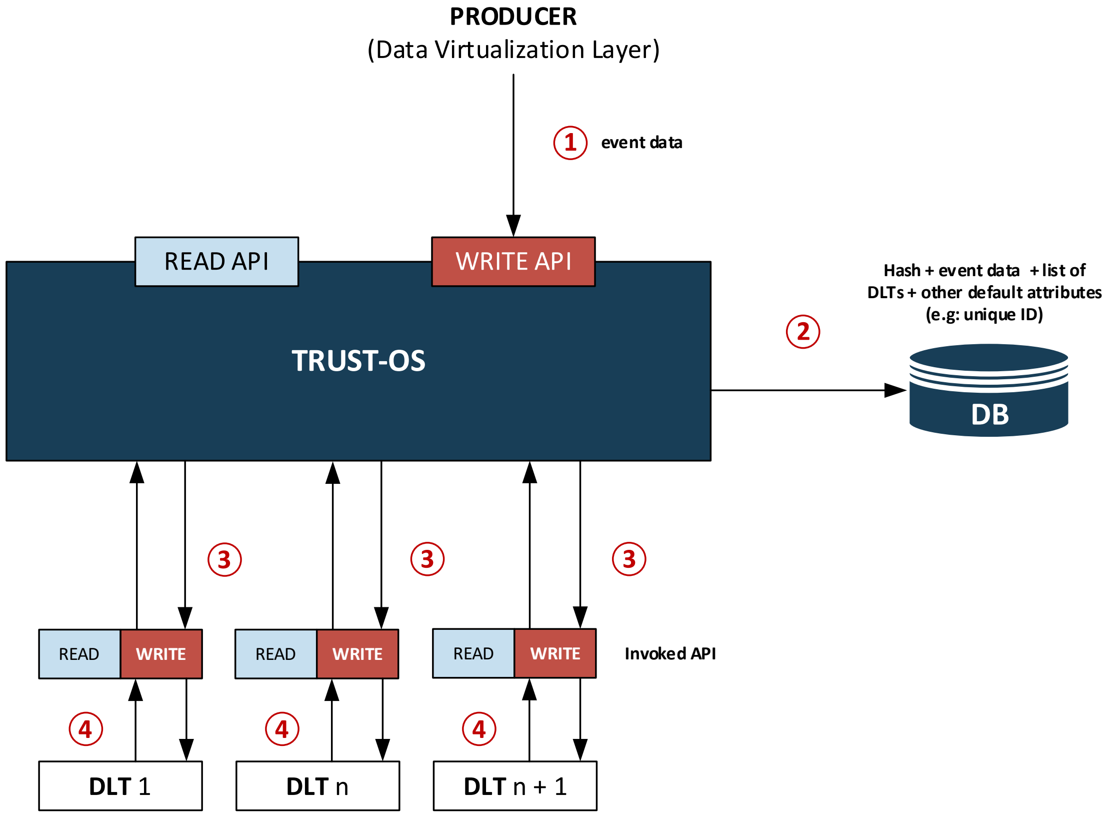


Figure 5.3: TrustOS and producer

The minimal viable solution is to provide the trusted storage mechanism that will guarantee immutability of the data. The immutability will be protected by the timestamp proof that consists of the timestamp data itself, and the hash of it stored in the hash tree, the root of which will be recorded on the DLTs. The Cross-DLT layer is composed of a set of APIs that access different DLTs.

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

These APIs will be developed by each partner and TrustOS will act as an orchestrator for these APIs as shown in Figure 5.3. The APIs will be specific to the underlying DLTs, but as similar to each other as possible in order to reduce the integration efforts. This architecture can be observed in Figure 5.3 and Figure 5.4, where there is a producer using the writing capabilities and a consumer using the reading capabilities, respectively. In the iNGENIOUS architecture, the producer is the Data Virtualization Layer, but it could also be an application from an upper layer as well as identified end users.

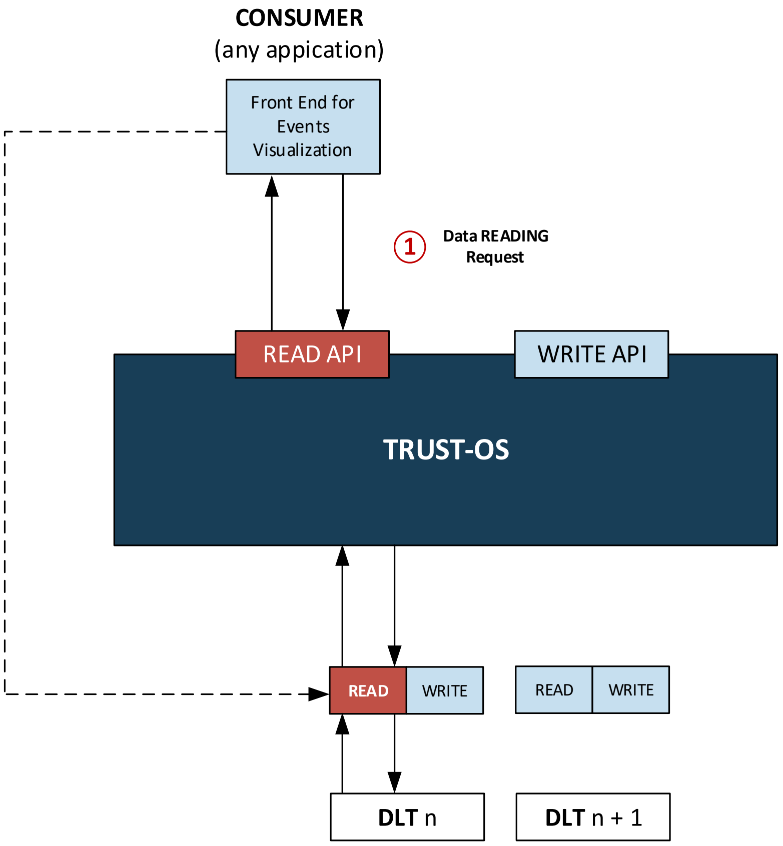


Figure 5.4: TrustOS and consumers

The consumer can interact with TrustOS in order to validate the proof-of-existence over their own data (through reading API) by trusting the interoperability layer. The dotted line in Figure 5.4 shows another method that the consumer can potentially use to verify the timestamp (in terms of inclusion proof) by connecting directly to the given DLT through a related API.

TrustOS will manage the hash trees for the data chunks that will be stored. The hash tree roots [18] will be sent to different DLTs in order to store them and protect from tampering. The consumer will be able to retrieve the inclusion proof from the TrustOS APIs. The producer will be verified by TrustOS to check if it is allowed to write data. The DLT APIs will receive write commands from TrustOS only.

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

The DLT API (connectivity) will be responsible to report the metadata that is required to identify the transaction with the given hash on the target DLT (for example transaction and block ID). It will also allow for fast search for the given hash (hash tree root) using transaction ID or hash itself. If the underlying DLT requires fees for performing transactions (like Bitcoin and Ethereum), then the DLT API will manage the wallet. The recommendation for the DLT API is to directly interact with a full node of the underlying DLT. The DLT connectivity APIs will be developed in a way that it will be easy to deploy new instances of them (for example – Docker).

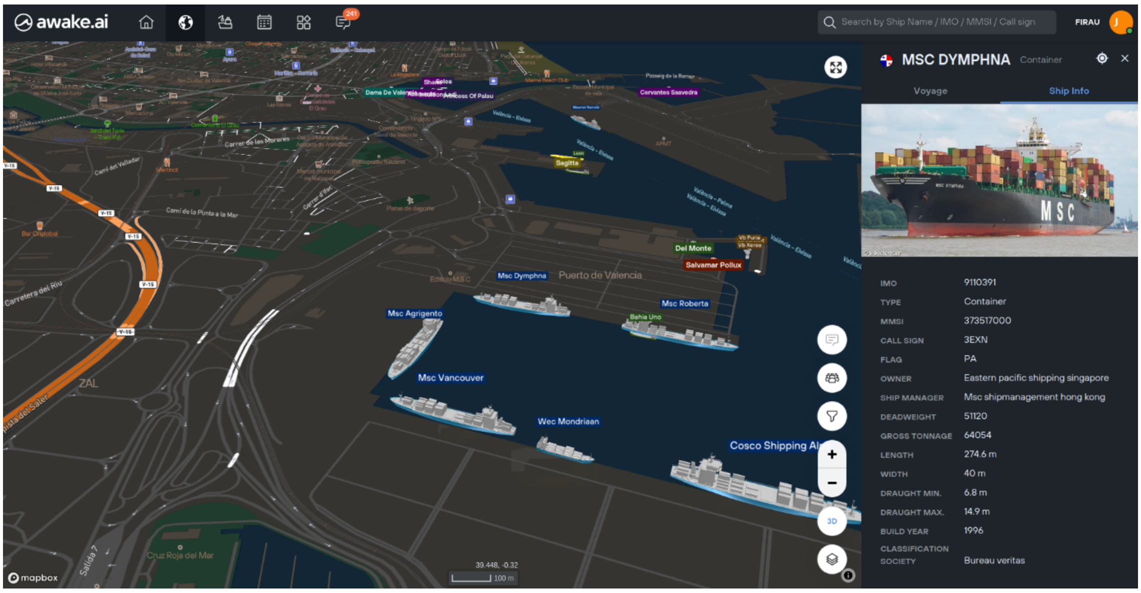
Component	Cross-DLT Layer	**Partner**	TID, CNIT, PJATK, FV
Use Cases	Port Entrance, Ship, DVL/DLT		
Key Innovation	One common mechanism for interacting with different DLTs Higher level of trust that stored data has not been altered (timestamp secured by the DLT) Better proof format that will allow for the verification on multiple DLTs		
Interfaces with	Data Virtualization Layer, DLT Solutions, Applications		

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

6 Application and Analytics Layer

The iNGENIOUS application layer uses Application Programming Interfaces (APIs) to access data from heterogeneous sources. These may include for example IoT devices and systems, logistic management systems, organizational information systems, and large-scale databases. The goal of such integration is to obtain a holistic view or situational awareness of events and processes related to selected application areas in the logistics chain. Using such holistic information, application-specific data analytics are developed, and their results provided for operational use through end-user applications.

The following section outlines the flow of data from IoT sensor devices to APIs for providing information to the application layer in the iNGENIOUS architecture. Subsequently, we describe how this data is used in offline machine learning model development to build predictive models, and how online services and applications will be developed to provide actionable insight for increased operational efficiency. Regarding data analytics and related end user applications, we focus here on the Port Entrance use case about situational understanding in smart logistics, where the goal is to improve the efficiency of a multimodal supply chain by automating the monitoring and schedule optimization of critical stages in land and sea logistics.



IMO	9110391
TYPE	Container
MMSI	373517000
CALL SIGN	3EXN
FLAG	PA
OWNER	Eastern pacific shipping singapore
SHIP MANAGER	Msc shipmanagement hong kong
DEADWEIGHT	51120
GROSS TONNAGE	64054
LENGTH	274.6 m
WIDTH	40 m
DRAUGHT MIN.	6.8 m
DRAUGHT MAX.	14.9 m
BUILD YEAR	1996
CLASSIFICATION SOCIETY	Bureau veritas

Figure 6.1: Awake.ai web application

As an example of the iNGENIOUS application layer, the Awake.AI web application (shown in Figure 6.1) will be integrated to heterogeneous maritime and port logistic data sources in the smart logistics use case to provide situational awareness of port operations and vehicle movements, and to visualize and communicate predictive analytics for operational optimization.

6.1 API for IoT Network Applications

An IoT network connects different devices and processing platforms. This creates rich resources for the development of applications. As illustrated in Figure 6.2, analogously to computer architecture, the IoT devices are the I/O, MECs play the role of CPU cores, and the network is the bus that connects all these devices. The management and orchestration play the role of the operating system. An application uses the services provided by the operating system and the device drivers to implement the end user functionality.

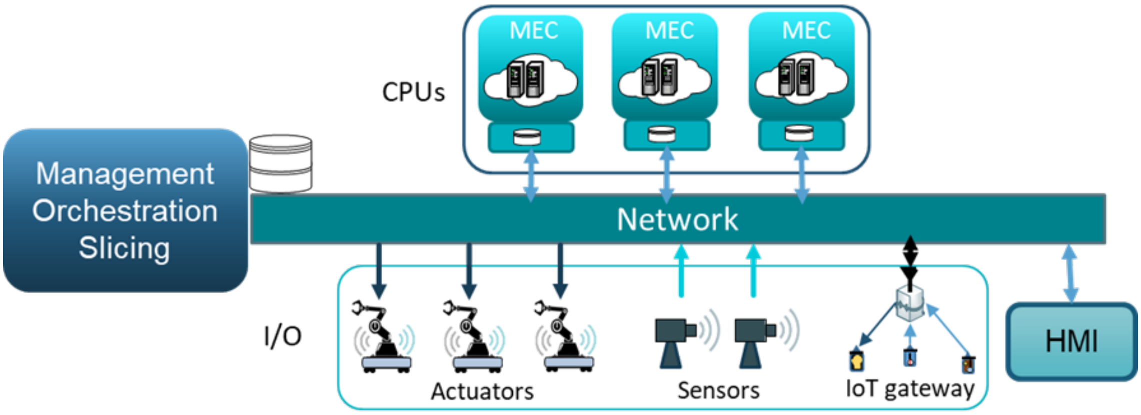


Figure 6.2: MEC-controlled IoT devices connected by networks

To facilitate application development for end users, it is necessary to provide APIs that abstract the underlying hardware. The purpose of an API is to provide an interface to the underlying resources which clearly defines the functionalities and data available for applications, is easy for application developers to work with, and does not allow misuse of the underlying resources. For example, a well-designed API should not allow access to data not meant for the API user or allow controlling actuators or sensor parameters in undesired ways.

Component	API for IoT Network Applications	**Partner**	TUD
Use Cases	Factory (demo)		
Key Innovation	Network as a distributed operating system with different levels of abstraction: APIs for end-user application development, APIs to abstract communication and data exchange with the IoT devices, and APIs to abstract network configuration and resource allocation based on the application E2E requirements		
Interfaces with	MANO, 5G Core Network		

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

6.2 Data Analytics

Using data analytics, iNGENIOUS will demonstrate how the efficiency of a multimodal supply chain can be increased by automating the monitoring and schedule optimization of critical stages in land and sea logistics. To do so, the project aims at designing a data analytics application layer able to exploit the potential provided by the data collected at the Data Management layer. Within the application layer, the project will leverage cloud computing, big data and machine learning techniques to extract knowledge from data collected in different supply chain processes using both offline and online analytics. iNGENIOUS will exploit the data analytics layer to predict and optimize truck turnaround times at port facilities by exploiting data obtained from different data sources like Gate Access systems, meteorological sensors, Automatic Identification Systems (AIS), Port Community Systems (PCS) and real-time IoT tracking devices.

The proposed data analytics layer will ingest data from the Data Virtualization Layer (DVL) and other external data sources like the PCS, AIS, etc. Application layer data analytics can be divided into two interdependent tracks: data analysis and model development based on historical data sets, and online services and application software providing inference results based on up-to-date data. These have different requirements in terms of the broader iNGENIOUS architecture, as the former requires querying large datasets compiled over time from heterogeneous sources, while the latter requires continuous ingestion of the most recent data from the corresponding sources.

In historical data analysis, after ingesting the data, the data analytics layer will first pre-process and transform all data flows to conform to a common data model and to filter out anomalous data points. After that, Exploratory Data Analysis (EDA) techniques will be carried out to label and subsequently identify cross-correlations between the ingested data flows. Once correlations are identified, the data analytics layer will exploit Machine Learning (ML) techniques for defining and training predictive data models. The choice of models will depend on the statistical characteristics and complexity of the processes to be optimized. After the training phase, models will be tested both statistically using dedicated validation and test sets and using simulations to estimate the effects of optimization models on target variables such as truck turnaround times.

Component	Data Analytics	**Partner**	AWA
Use Cases	Port Entrance (demo)		
Key Innovation	Building predictive models for port logistic processes and traffic patterns using heterogeneous data sources provided by the iNGENIOUS architecture		
Interfaces with	Data Virtualization Layer		

6.3 Applications

This section summarizes the applications that the iNGENIOUS architecture enables, and the user interfaces developed in the project.

6.3.1 SMART AND TACTILE IOT APPLICATIONS

The IoT Network APIs allow dynamic reconfigurations of the network resources to implement customized applications. An application is composed of closed-loop control threads that involve sensors, actuators, and controllers running on one or more MEC. In addition, a human operator can interact with the application by means of a user interface, which can be a tactile human-machine interface (HMI) or a web application. The APIs provide several interfaces including E2E requirements configuration, processing algorithms deployment, data communication between devices, user monitoring and control interface. Accordingly, the network resources include sensors/actuators and other computation and storage devices in the network which can be programmed to perform different tasks. In particular, iNGENIOUS focuses on applications in industrial networks such as teleoperation, autonomous driving, mobile robots, and industrial automation.

6.3.2 SMART LOGISTICS APPLICATIONS

The implementation of online services and application software for data analytics will take advantage of the existing Awake.AI platform, which provides fully cloud-based Kubernetes environments with existing microservices for data ingestion, predictive analytics, geodata visualizations, communications, web and mobile applications, and external API access. These will be used to interface with relevant components in the overall iNGENIOUS architecture to obtain necessary input data and apply the prediction and optimization models developed in historical data analysis. Communication services and API access can be used to provide the output data either to end users directly, or to external port information systems to manage resource more efficiently.

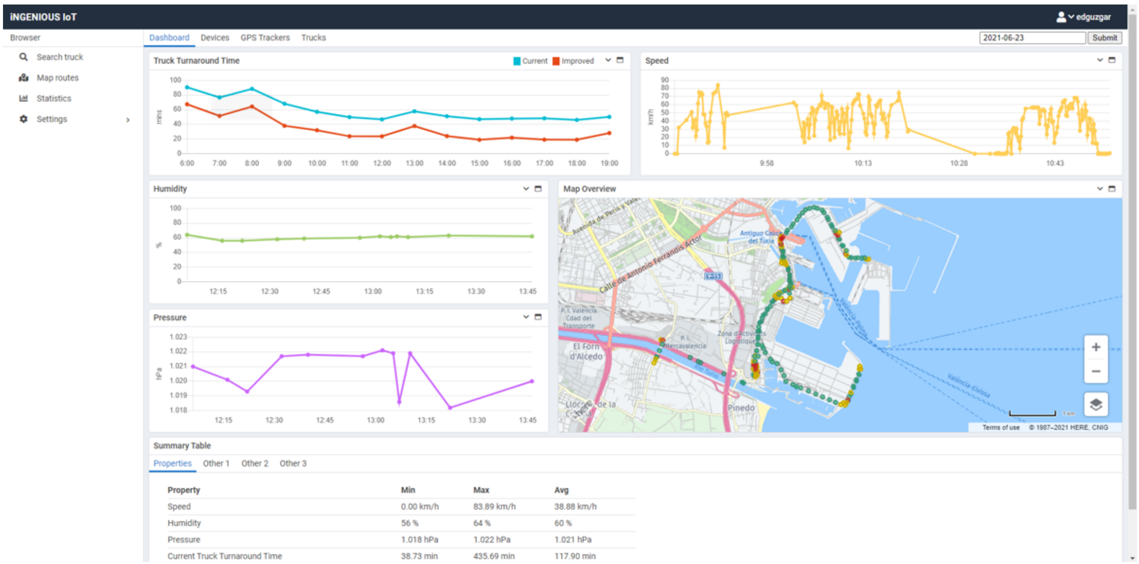
6.3.3 VISUALIZATION TOOLS

A dashboard has been developed to visually show historical and real-time tracking data at the port of Valencia and Livorno for the Port Entrance use case. Using the tracking data, the truck turnaround time will be calculated and shown in a graph, and temperature, wind and humidity data from the Valencia port meteorological station will be included in the future using the PI System OSIsoft M2M platform.

The map API used is Here Maps API, and when a truck enters the port, its position and speed is sent to a server every 10 seconds, which is then represented in the map using three different colors. The red color represents speeds lower than 20 km/h, the yellow color represents speeds between 20 and 35 km/h and the green color is shown when the speed is higher than 35 km/h. This

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

color palette will be useful to locate the bottlenecks and crucial spots inside the ports by visualizing the problematic zones.



Property	Min	Max	Avg
Speed	0.00 km/h	83.89 km/h	38.88 km/h
Humidity	56 %	64 %	60 %
Pressure	1.018 hPa	1.022 hPa	1.021 hPa
Current Truck Turnaround Time	38.73 min	435.69 min	117.90 min

Figure 6.3: Dashboard for Valencia port

Geofences are geographical polygons which can be used to delimit certain areas. They have been used to delimit the port area, to avoid storing coordinates of the trucks outside the port. Furthermore, they are used to change the reporting frequency of the trackers, which may send data only every 10 minutes to lower their energy consumption. Inside the port, different geofences are used to store crucial events, like port entrance or exit, or also to calculate the transition time between different spots inside the port (e.g., measuring queuing times the queue at the port entrance).

Additionally, the Awake.AI web application shown in Figure 6.3 on page 61 provides visualizations for global vessel traffic (map views showing vessel locations, predicted routes, navigational and port-related geofences, etc.), port schedule timelines, gate traffic information (truck and container entry/exit events and statistics), weather information, and communication tools such as port call-specific chat rooms supporting automated communication of detected events such as vessel geofence entries.

Component	Applications		**Partner**	AWA, UPV
Use Cases	Factory, Port Entrance (demo)			
Key Innovation	Deeper integration with network infrastructure for applications based on smart IoT network APIs Communicating predictions and recommendations to logistic operators through end user applications in order to improve operational efficiency			
Interfaces with	Data Analytics, Data Virtualization Layer, other external data sources			

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

7 Conclusions

The D2.2 deliverable provides an overview of the initial system and architecture integration in iNGENIOUS. The four main Chapters 3 through 6 explain all components and their interrelationships within the cross-layer architecture. Thus, it can serve as a reference document and record of common understanding of the iNGENIOUS architecture, which will continue to guide the activities in the technical work packages.

This version of the document summarizes the results of task T2.2 until month M14. The consortium partners will jointly work on further refining this initial architecture description. In particular, as the technical work progresses, the project partners intend to provide information on the interfaces and cross-layer interactions among the components in the follow-up deliverable *D2.4 System and architecture integration (final)*, which will be released in month M24.

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

References

[1] “iNGENIOUS deliverable "D2.1 Use cases, KPIs and requirements",” 2021.

[2] “iNGENIOUS deliverable "D5.1 Key technologies for IoT data management benchmark",” 2021.

[3] Wikipedia, “Design of experiments,” [Online]. Available: https://en.wikipedia.org/wiki/Design_of_experiments. [Accessed 28 March 2021].

[4] “iNGENIOUS deliverable "D3.1 Limitations and improvement axis for the communication of IoT devices",” 2021.

[5] 3GPP, “TR 37910 - Study on self evaluation towards IMT-2020 submission,” 2019.

[6] 3GPP, “RP-193264: Rel-17 enhancements for NB-IoT and LTE-MTC,” 2019.

[7] 3GPP, “RP-193235: New Rel-17 SI for NB-IOT/eMTC over NTN,” 2019.

[8] 3GPP, “RP-193233: New WID on enhanced Industrial Internet of Things (IoT) and URLLC support,” 2019.

[9] 3GPP, “RP-193238: New SID on Study on support of Reduced Capability NR Devices,” 2019.

[10] “iNGENIOUS deliverable "D4.1 Multi-technologies network for IoT",” 2021.

[11] 3GPP, “TS-36300: Evolved Universal Terrestrial Radio Access (E-UTRA) and Evolved Universal Terrestrial Radio Access Network (E-UTRAN)”.

[12] H. Hu and J. Zhang, “Self-Configuration and Self-Optimization for LTE Networks”.

[13] J. Ali-Tolppa, S. Kocsis, B. Schultz, L. Bodrog and M. Kajo, “Self-helaing and resilience in future 5G cognitive autonomous networks”.

[14] 3GPP, “TR-28861: Study on Self-Organizing Networks (SON) for 5G,” 2018.

[15] O-RAN Alliance, “O-RAN Architecture Description,” 2020.

[16] oneM2M, “oneM2M - Standards for M2M and the Internet of Things,” [Online]. Available: https://www.onem2m.org/technical/partner-transpositions. [Accessed March 2021].

[17] P. Todd, “OpenTimestamps: Scalable, Trust-Minimized, Distributed Timestamping with Bitcoin,” 2016. [Online]. Available: https://petertodd.org/2016/opentimestamps-announcement.

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

[18] R. Merkle, “Protocols for Public Key Cryptosystems,” in *1980 IEEE Symposium on Security and Privacy*, Oakland, CA, USA, 1980.

[19] J. Blackman, “Enterprise IoT Insights,” 2019. [Online]. Available: https://enterpriseiotinsights.com/20191016/channels/fundamentals/what-is-mmtc-in-5g-nr-and-how-does-it-impact-nb-iot-and-lte-m.

[20] 3GPP, “TR-22836: Study on asset tracking use cases,” 2018.

[21] 3GPP, “RP-202933: Support of reduced capability NR devices”.

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