NEXT GENERATION INTERNET

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

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

D2.4 System and Architecture Integration (Final)

Revision: v1.0

Work package	WP 2
Task	Task 2.2
Due date	30/09/2022
Submission date	30/09/2022
Deliverable lead	Barkhausen Institut (BI)
Version	1.0
Authors	Manuel Fuentes (5CMM), Miguel Cantero (5CMM), Luis Cascajar (ASTI), Manuel García (ASTI), Jussi Poikonen (AWA), Carsten Weinhold (BI), Jose Costa-Requena (CMC), Alexandr Tardo (CNIT), Eddy Higgins (iDR), Joe Cahill (iDR), Shane Bunyan (iDR), Clemens Saur (NCG), Nuria Oyaga (NOK), Erin Seder (NXW), Giacomo Bernini (NXW), Pietro Piscione (NXW), Tadeusz Puźniakowski (PJATK), Efstathios Katranaras (SEQ), Christos Politis (SES), Juan Jose Garrido Serrato (SES), Cesar Rodriguez Cerro (TIOTBD), Ivo Bizon (TUD), Rania Rojbi (TUD), Raul Lozano (UPV)
Reviewers	Nuria Molner (UPV), José Luis Cárcel (FV), Marek Bednarczyk (PJATK), Efstathios Katranaras (SEQ), Gino Ciccone (TEI)

Abstract	This document provides an overview of the iNGENIOUS cross-layer architecture. The focus is on component groups within the overall architecture and how their integration and cooperation enable the related iNGENIOUS innovations.
Keywords	INGENIOUS, architecture, vertical, cross-layer

Document Revision History

Version	Date	Description of change	List of contributor(s)
V1.0	30/09/2022	EC version	See author list

Disclaimer

This iNGENIOUS D2.4 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 Final Review Meeting planned in July 2023, 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. An initial version of the architecture has already been presented in deliverable **D2.2 System and architecture integration (Initial)** [1]. While D2.2 mostly described the individual technological building blocks, this updated deliverable focusses on the interaction of components and how their cooperation enables the key innovations of the iNGENIOUS project.

This document first describes the architecture from a high-level point of view and thereby summarizes 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 describe a total of nine component groups. Each of these component groups represents a part of the architecture, for which the state of the art before iNGENIOUS is summarized and how integration of novel and enhanced components brings technical and business innovation to the next-generation IoT-based supply chain and logistics.

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

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
NB	Narrow Band
NFV	Network Function Virtualization
NG	Next Generation

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

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

Before discussing the iNGENIOUS cross-layer architecture itself, we explain its role within the project. We then describe how we chose to structure the content in order to help the reader get an overview quickly, but also find sufficient detail within this document as well as the deep dives in the other deliverables (both technical and exploitation related).

1.1 Role of Task T2.2 in iNGENIOUS

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. The use cases are described in detail in deliverable **D2.1 Use cases, KPIs, and requirements** [2] . We summarize them here to make clear what the goals of the project are and what areas must be covered by the iNGENIOUS overall architecture.

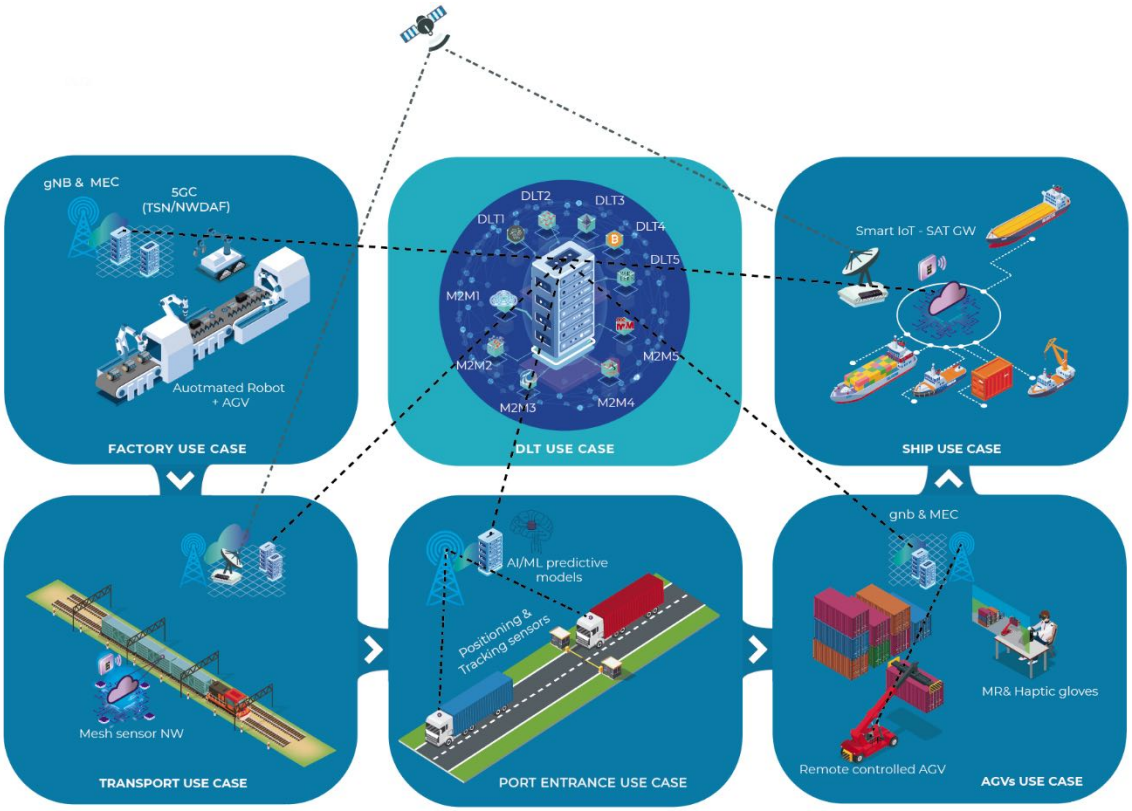

Figure 1:1: The six use cases of the iNGENIOUS project covering the supply chain and data management.

Use Case Requirements: 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 cover all parts of the supply chain. We start right in manufacturing (*Factory* use case), where automated robots increase efficiency by working fully autonomously or by assisting human workers. To innovate transportation logistics, IoT sensors shall monitor the safety-critical parts of land-based transport vehicles. These smart sensors enable longer maintenance intervals that help reduce costs, while ensuring reliable detection of defects that could otherwise lead to accidents (*Transport* use case). By integrating

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

network technologies ranging from local-area wireless networks all the way up to satellites, the project aims to enable in the *Transport* and 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 5G networks to remotely control vehicles in situations where humans would be in danger or exposed to adverse environmental conditions (*AGV* use case).

Enabling the Use Cases: As goods and vehicles move along the supply chain, data needs to be collected, transmitted, and processed to enable these new use cases or optimize already established ones. The iNGENIOUS architecture is therefore a *data-driven architecture*. This aspect is covered by the *DVL/Cross-DLT* use case, which connects physical parts of the supply chain at the data level and enables comprehensive tracking and optimization. This use case aims to integrate the various data flows into a comprehensive data management and analytics framework, while providing important functionalities to ensure that supply-chain data is secure.

Key principles to enable the combination of the 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 of the technology stack. 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* in addition to enabling the data flows.

1.2 Navigating this Document

This deliverable gives an overview of the technical work in iNGENIOUS. It concentrates on the interaction of key components within the cross-layer architecture. Those interactions are described in their own sections, which are structured as shown in Table 1 and explained in the paragraphs that follow.

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

Section numbering		Title and content
X.Y		**Component group: *<Comp1>*, *<Comp2>*, and *<Comp3>*** Brief introduction of the components *<Comp1>* through *<Comp3>* that form the group and their role within the architecture.
	X.Y.1	**State of the Art before iNGENIOUS** Brief summary of the state of the art related to *<Comp1>* through *<Comp3>* before the project.
	X.Y.2	**iNGENIOUS Contribution and Innovation** Innovation table that briefly summarizes key innovations, both individually for *<Comp1>* through *<Comp3>* and as a result of their integration in iNGENIOUS. In the text we highlight how the integration of the components in the iNGENIOUS architecture is more than the sum of its parts.
	X.Y.3	**Use Case Coverage and Exploitation Potential** Coverage and exploitation table that: • Maps components *<Comp1>* through *<Comp3>* to the use cases • Maps the integrated group of components to the testcases, which in turn are based on user and system requirements • Highlights exploitation/business potential enabled by iNGENIOUS innovations for this component group

Table 1: Structure of the main sections that describe component groups

The purpose of the **first subsection** is that we can better point out in the following subsection how the components and their integration enable the iNGENIOUS innovations.

In the **second subsection**, we give bullet points to summarize in a table the key innovations. Technical details, but in a short and concise form, are explained in the text following this table. To avoid duplication of content, we summarize the most important technical aspects needed to explain cooperation and integration of the components. We point to technical deliverables D2.x, D3.x, D4.x, D5.x, and D6.x for all the details beyond this overview.

Likewise, details about exploitation will be in presented in deliverable **D7.3 Final dissemination, standardization and exploitation** [3], but we summarize them as bullet points in the table in the **third subsection**, such that the relevance of the innovations can be assessed more easily. There, we also list use-case and test-case coverage relevant to the component group.

Cross-document references: Cross references to other deliverables are done by explicitly naming the number and title of the referenced deliverable (as for D7.3 above) and the bibliography link. If appropriate, we also point the reader to specific sections within that deliverable. Another important type of cross-references are the identifiers used to designate test cases and requirements defined in other deliverables. To interpret them correctly, we refer the reader to the following note and mapping table.

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

Note: At the time of submission of deliverable **D2.1 Use cases, KPIs and requirements** [2], the project had not yet established unique identifiers, like for example UC1_SR_10, which refers to system requirement #10 of the Factory use case. However, the requirements in D2.1 are numbered accordingly. To help the reader map test cases to system requirements (which are in turn derived from user requirements), the following rows of this table list the use-case-to-identifier mappings.	
Use Case Name	**System Requirements and Test Case Identifiers**
Factory	UC1_SR_x, UC1_TC_x
AGV	UC2_SR_x, UC2_TC_x
Transport	UC3_SR_x, UC3_TC_x
Ship	UC4_SR_x, UC4_TC_x
Port Entrance	UC5_SR_x, UC5_TC_x
DVL/DLT	UC6_SR_x, UC6_TC_x

Document Structure: The document as a whole is structed as follows: Chapter 2 consists of a high-level description of the architecture. Chapter 3 covers three component groups in the things layer that are subject of the research in WP3 of the project. Chapter 4 describes the two most important groups of network components from WP4. Component groups that enable key iNGENIOUS innovations in the data management layer are described in Chapter 5, followed by two more groups innovating applications and data analytics in Chapter 6. Both of these chapters cover WP5. Chapter 7 ends the architecture discussion by highlighting use case coverage of all components. Chapter 8 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. They cover – from bottom to top – IoT devices (or "things"), network infrastructure, data management and analytics, and applications. We previously described these layers in **Chapter 2** of iNGENIOUS deliverable **D2.2 System and architecture integration (Initial)** [1]. For completeness and to provide a high-level overview, we include an updated version of this description in the following sections of this chapter.

2.1 IoT Things Layer

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.

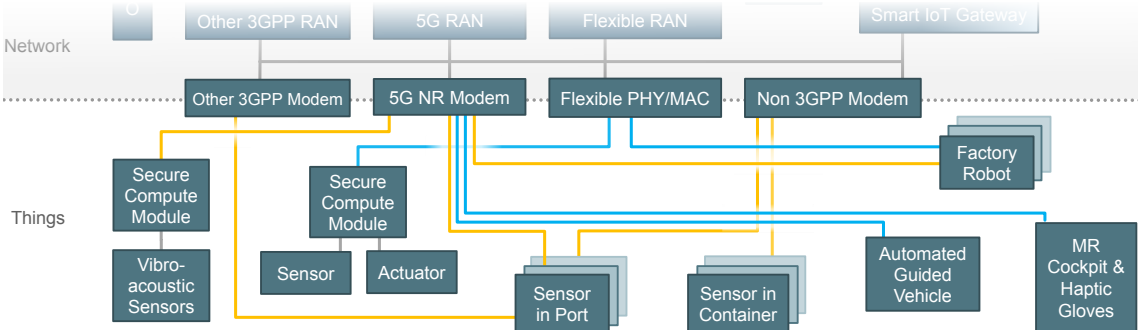

Figure 2:1: IoT devices in the iNGENIOUS architecture for all use cases considered in the project.

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).

2.2 IoT Network Layer

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.

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

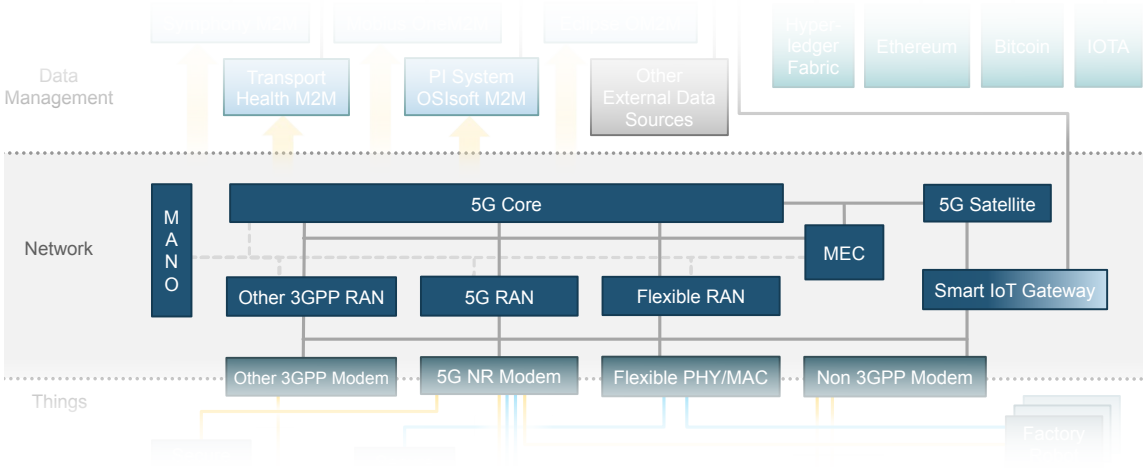

Figure 2:2: Network layer of the iNGENIOUS architecture.

This layer also includes non-3GPP networks, some of which are integrated into the architecture via a smart IoT gateway. Furthermore, iNGENIOUS partners contribute Radio Access Technology (RAN) that supports flexible PHY/MAC implementations. 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.

2.3 Data Management & Application Layers

IoT devices not only differ in terms of RAN, 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

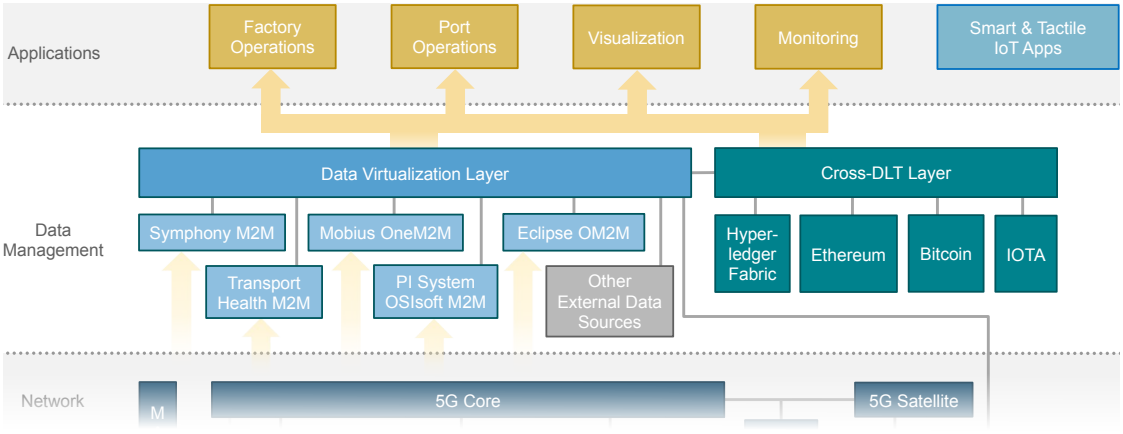

Figure 2:3: Data management and analytics layer of the iNGENIOUS architecture for applications considered in the project use cases.

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

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

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.

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 in Figure 2:4.

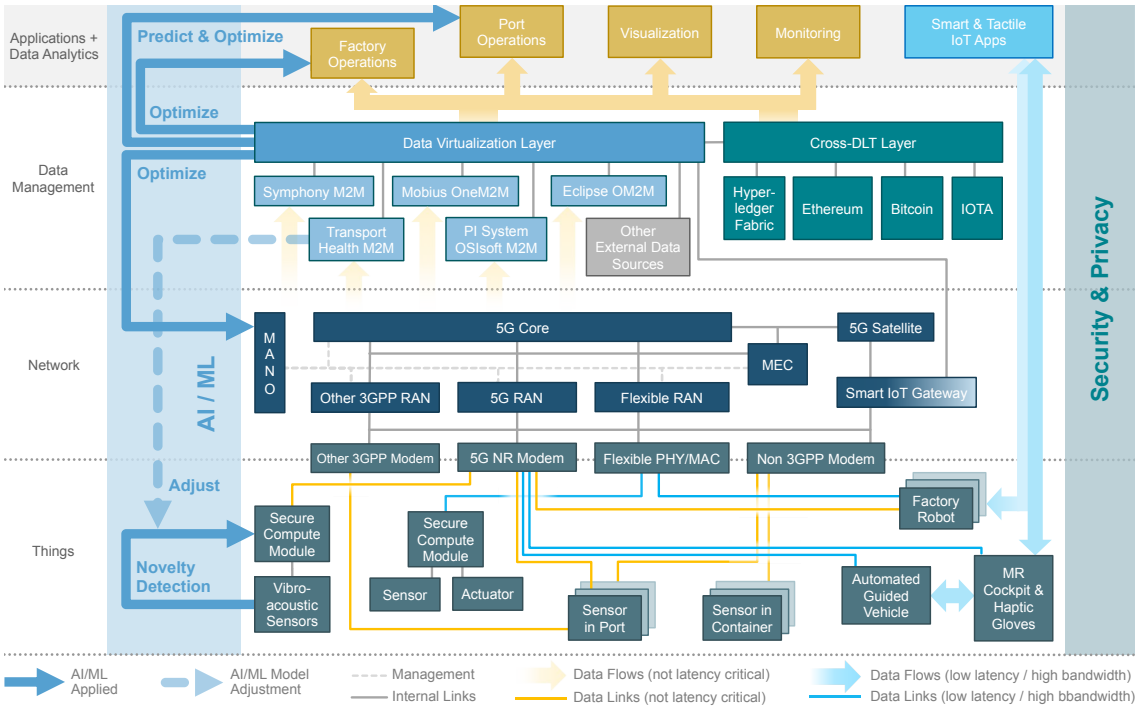

Figure 2:4: Complete iNGENIOUS architecture with all components and the interaction between them.

2.4 Cross-Layer Interaction

The yellow lines and 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 blue links 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. This is not highlighted in the figure for readability reasons, but the light-blue arrows on the right side show between which components the bandwidth and latency guarantees must be met end-to-end and across layers. 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.

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

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.

AI/ML as a Cross-layer Concern: 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-around times in the ports. Additionally, 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 ML processing capabilities that enable the Transport use case.

Security as a Cross-layer Concern: 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** [4]. 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 employs 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.

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

3 IoT Device Layer

The lowest level within the iNGENIOUS IoT system architecture is the IoT device layer, which includes the "things" that interact with the physical world. Primarily, these things are:

a. *Edge sensors*, for asset tracking and monitoring
b. *Actuators,* such as Automated Guided Vehicles (AGVs) and automated robots, for logistics transportation in maritime ports and terminals or distribution in smart factories
c. *Immersive devices,* such as mixed reality glasses and haptic devices, for enabling the remote controlling of automated actuators in real-time with human feedback

To become IoT devices and data originators, these entities require embedded compute units and communication hardware and software that connect them securely to a network. iNGENIOUS evolves the hardware and software architectures of the various parts of the IoT devices, as well as their connectivity solutions, in order to address the identified current limitations and ease their adoption in the selected use cases. The following evolution of components and their interactions are described in this chapter:

- *Edge sensors and Compute Platform*
  - Neuromorphic context-based edge clustering, situational edge computing, and efficient monitoring for optimized cost energy and use case feasibility.
  - Secure-by-default hardware/software architecture 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.
- *Flexible PHY/MAC and Compute Platform*
  - FPGA implementation of different software-defined flexibility levels at compile-time and run-time for customization and optimization to specific IoT air interfaces as well as to support for different traffic classes.
  - Deployment of baseband processing and utilization of secure-by-default architecture for secure data transfer at physical layer.
- *Immersive devices, AGVs, and 5G modem*
  - *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
  - Compact, Low-Power, and Customizable 5G modem for flexible and "plug and play" 5G wireless connectivity experience
- *Other components*
  - Considerations for modem feature implementations and air interface solutions to lower the cost of communication in terms of computational complexity, power consumption, latency, flexibility.

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

In this chapter, we introduce the diverse device components which iNGENIOUS will evolve and leverage for its use cases. For each component, the State of the Art before iNGENIOUS is provided and we elaborate on the iNGENIOUS contribution and innovation along with the respective use case coverage and exploitation potential.

3.1 Component Group: Edge Sensors and Compute Platform

Sensors and actuators become IoT devices only by connecting them to a network, so that they can send measurements to control systems or receive commands from them. To enable this cooperation, edge sensors and actuators need local compute capacity to run communication protocols as well as cryptographic algorithms to protect control messages and data sent through the communication links.

In this section, we describe a component group consisting of a smart edge sensor for rail-carriage monitoring and a generic computer platform, highlighting the efficiency and security benefits of their integration in the Transport use case.

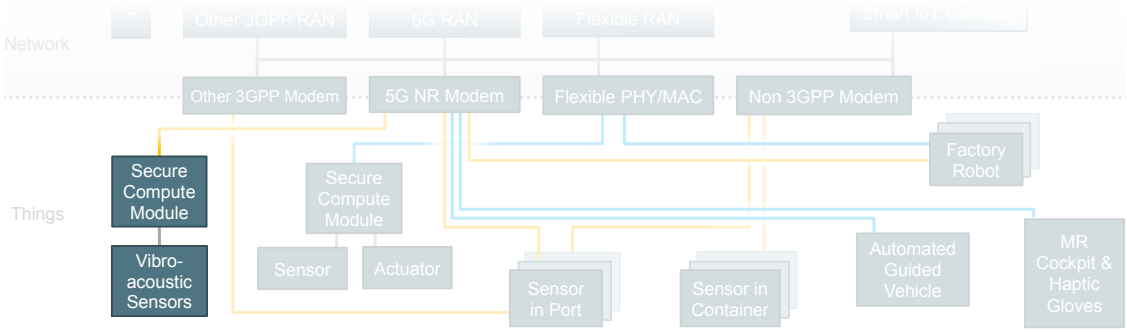

Figure 3:1: Secure compute platform and edge sensors in architecture

3.1.1 STATE OF THE ART BEFORE INGENIOUS

Parts of the supply chain are land-based transport vehicles. Cargo train carriages are of particular importance in logistics and reducing the cost of operating them is a key business goal. To meet safety requirements and to avoid costly accidents, the carriages require preventive maintenance in regular intervals. But these inspections come at a cost, as they cause downtime, even though the majority of cargo carriages did not develop any safety-critical defects. Reducing these costs by increasing maintenance intervals is only possible, if there is a lower-cost way to detect the rare occurrence of defects in the small subset of carriages that could indeed cause an accident.

Currently, there are no low-power edge sensors capable of permanent monitoring of train-health conditions that meet cost, power, energy, and longevity targets. A key problem is that these sensors must communicate to report detected problems, but communication requires energy. Autonomous processing at the edge can help reduce the need for frequent communication and transmission of large amounts of data. **Section 3.1** of deliverable **D3.1**

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

Limitations and improvement axis for the communication of IoT devices [5] discusses the problem and state of the art in greater detail.

The other problem is IoT device security. IoT devices run large amounts of complex software that implement communication protocols. This complexity is required for the edge device to fulfil its purpose, but it is also the enemy of security and reliability. In general, the embedded computers of edge devices are critical for the trustworthiness of the IoT system as a whole. In the context of the iNGENIOUS Transport use case, the safety of trains directly depends on IoT device security. Therefore, it is important that the on-device software is structured in such a way that security risks are minimized.

However, IoT computer architectures and operating systems typically fall short on this requirement because they are complex and architected such that both failures and attacks can compromise an IoT device with relative ease. More secure and efficient architectures exist but are not widely deployed in IoT scenarios. Thus, currently available IoT systems are unfit for the ever-increasing dependence on security and safety-critical IoT sensors and actuators. A detailed discussion and review of the state of the art in IoT computer security can be found in **Sections 3.3 and 3.4** of deliverable **D3.1 Limitations and improvement axis for the communication of IoT devices** [5].

3.1.2 INGENIOUS CONTRIBUTION AND INNOVATION

A high-level description of the two components in this component group, *Edge Sensors* and *Highly-secure and Low-power Compute Platform*, can be found in **Sections 3.1** and **3.2**, respectively, of **D2.2 System and architecture integration (Initial)** [1]. Here, we focus on how they integrate and the innovation this brings to the project's Transport use case.

Innovation Summary: Edge Sensors and Compute Platform
Edge Sensors: • 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 **Compute Platform:** • Secure-by-default computer and operating-system architecture • Hardware root of trust for remote attestation of device integrity • End-to-end secure communication and authentication **Benefit due to integration of the components:** • Low-power condition monitoring and reporting • Stronger security guarantees for edge-cloud communication

Smart edge sensors can reduce overall energy consumption, if one can optimize the Cloud-Edge paradigm. Under this paradigm, communication costs for offloading to the cloud are traded against cost of local computation capacity, as shown in Figure 3:3:

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

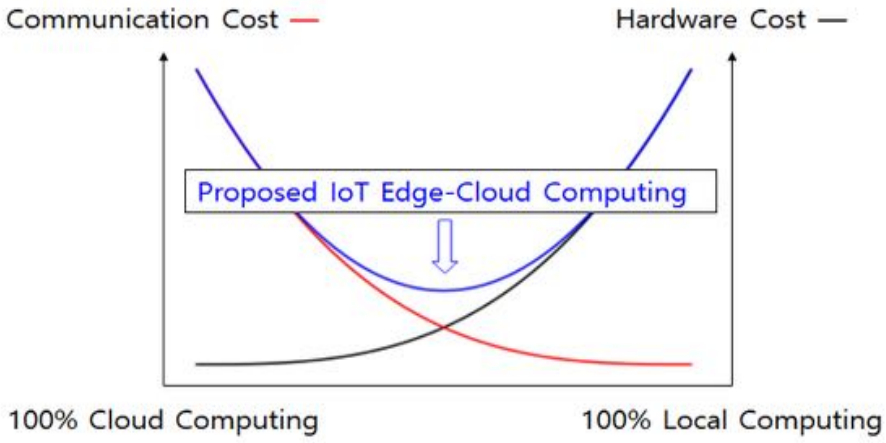

Figure 3:3: Cost for communication needed to offload vs. hardware cost for local computing

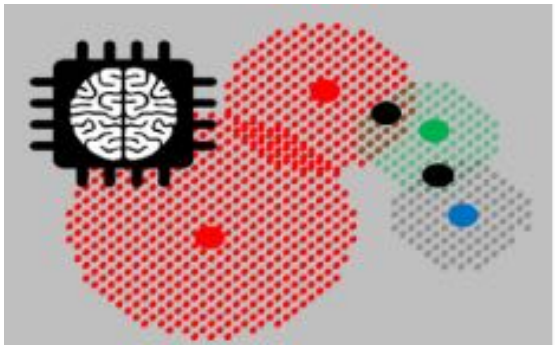

Figure 3:2: Neuromorphic Clustering (Known Clusters & Unoccupied Feature Space)

The innovation in edge sensors from iNGENIOUS 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. For the Transport use case, NeuroControls (NCG) performed edge data collection for ML-based condition monitoring using real cargo train carriages on a test track. The core approach is to continuously monitor the axles of the carriages using vibro-acoustic sensors. Processing the sensor data is performed at the edge (i.e., on the train) with the goal to categorize observed sensor readings into clusters, which are known to represent certain types of defects in wheels and bearings, according to an edge data collection campaign (see Figure 3:2 below). When sensor readings fall into a cluster that represents a potentially safety-critical defect, an alert must be sent to a remote monitoring data centre using wireless communication. A complete discussion of this approach to edge sensors in iNGENIOUS can be found in **Section 2** of deliverable **D3.3 Secure, private and more efficient HW solutions for IoT devices** [6].

The communication between the Edge sensor and the control centre is security critical for two reasons:

1. It must be ensured that the control centre will only process genuine sensor readings. Falsified status message could lead to unnecessary

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

downtime (“false defect”), prevention of necessary maintenance (“false OK”), or other attacks on safety and availability of the train carriage.

2. The edge sensor device must be certain that it is indeed communicating its reports to a genuine control centre and not to a server that is under control of an attacker. This is important to ensure confidentiality of reports, but also to make sure that commands and configuration updates received by the edge device are indeed coming from the legitimate control centre operated by the owner of the train carriages.

To achieve secure communication as described above, the IoT device’s operating system (OS) and the embedded computer hardware must provide security mechanisms to protect device-specific software and state. The device must also support strong authentication and integrity verification of the respective communication partner at the other side of a cryptographically protected communication channel. To this end, Barkhausen Institute (BI) contributes to the iNGENIOUS architecture a microkernel-based OS called M³ 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, M³ applies the same isolation-by-default approach to hardware as shown in Figure 3:4.

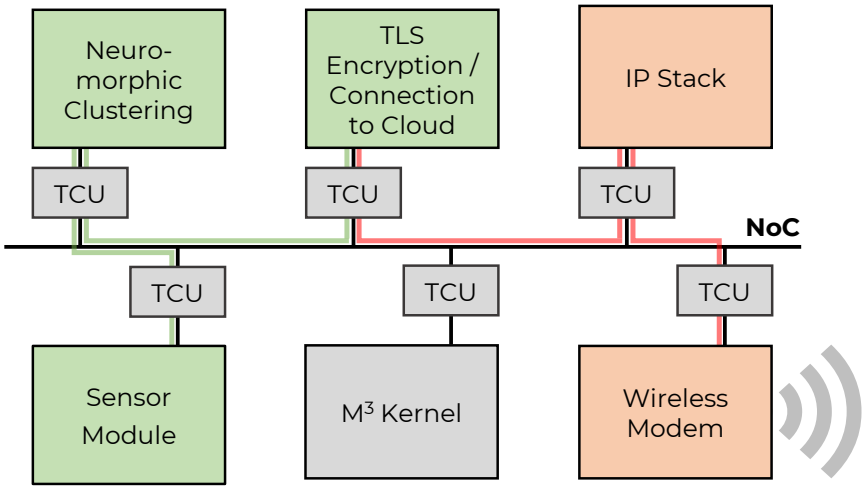

Figure 3:4: M3-based platform with integrated neuromorphic sensor tiles and wireless modem

In this architecture, processing tiles are connected to a network on chip (NoC), which enables cooperation among software components running on these tiles. But a small hardware component called Trusted Communication Unit (TCU) between each tile and the NoC can also enforce isolation in hardware, thereby implementing access control and data-flow policies. **Deliverable D3.3 Secure, private and more efficient HW solutions for IoT devices** [6] describes the OS and hardware architecture, I/O device support, and security

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

properties in full detail. In a nutshell, access-control enforcement by the TCU allows system designers to integrate and police tiles with general-purpose processors (i.e., those that run software). But also hardware accelerators 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.

The envisioned integration of edge sensors with local processing capabilities into the M³ platform is shown in Figure 3:4. The sensor module in the bottom left provides data from an externally connected vibro-acoustic sensor. The neuromorphic clustering happens on the top-left tile in diagram. The configuration of the green and red data-flow channels between the tiles enforces encryption, integrity protection, and authentication for all communication with the server in the remote control centre, as processed sensor reports can only pass through the TLS (Transport Layer Security) component. A minimal Root of Trust (RoT), which is integrated into the hardware, and corresponding OS support in M³ enable remote attestation together with TLS.

3.1.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

Component Group: Edge Sensors, Compute Platform

Relevant for use cases: Transport

Evaluation use case: Transport

Test cases: UC3_TC_01, UC3_TC_02, UC3_TC_04, UC3_TC_06 – UC3_TC_14, UC3_TC_20

Exploitation Potential:

- **NCG**, as a small/medium business, targets low-power, long lifetime vibro-acoustic edge sensors with Bluetooth Low Energy (BLE) connectivity for mobile and industrial applications. The ultimate goals are a smart bolts with vibration-based energy harvesting, sensing, computation, and secure connectivity (Condition Monitoring), and an intelligent data logger for accelerated data science with diverse balanced neuromorphic data cluster (Test System). The field of applications for condition monitoring focusses on transport and logistics, automotive, industrial, infrastructure. The field of applications for test systems focuses on Product Validation Testing and Industrial.
- **BI**, as an academic research institute, will exploit iNGENIOUS-funded developments of its platform for teaching and as a basis for future research and collaborations. Parts of the BI compute hardware and operating system platform are already open source and therefore available to academia and industry; more components shall become open source as research and development progress.

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

3.2 Component Group: Flexible PHY/MAC (UE Side) and Compute Platform

In this section, we describe the flexible PHY/MAC component implementation running on software-defined radio (SDR) equipment, highlighting the potential benefits of its integration with BI's compute platform in the Factory UC.

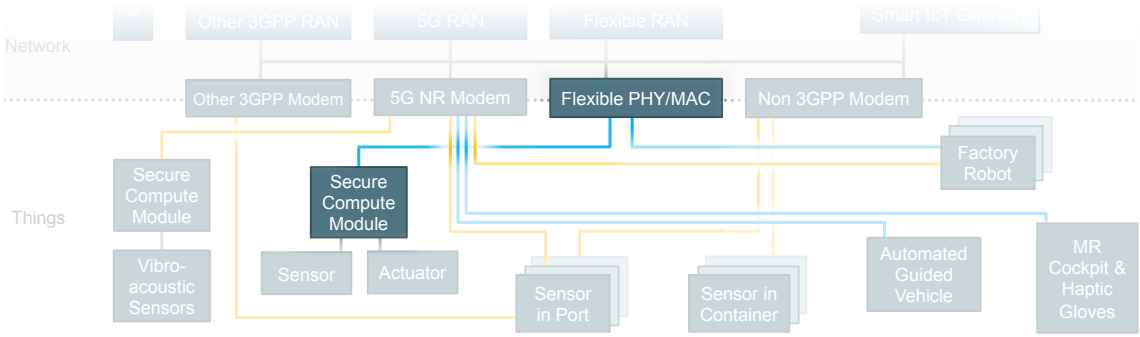

Figure 3:5: Component group consisting of flexible PHY/MAC and secure compute platform

3.2.1 STATE OF THE ART BEFORE INGENIOUS

The implementation of physical layer (PHY) signal processing algorithms of the transceiver chain is required to run in real-time. This goal can be achieved by employing application-specific integrated circuits (ASICs), field-programmable gate arrays (FPGAs), or software defined radio (SDR) baseband processors. ASIC implementation offers the best performance in terms of computing capacity and energy efficiency. However, this comes at the price of a lack of flexibility and a long development cycle. Once an ASIC is developed for a certain task, updates cannot be made. Unlike ASICs, an FPGA can be reprogrammed and still provide comparable computing performance. FPGA flexibility comes at the cost of a higher power consumption. The aforementioned approaches rely on hardware development, which on one hand provide high performance and efficiency, but on the other hand lack the flexibility of function reconfiguration [7] [8]. Software defined radio (SDR) enables the development of reconfigurable wireless systems that run in a generic programable platform, and PHY functions are executed on a general-purpose processor. This motivates the development of a PHY framework that can be implemented on efficient hardware, and at the same time present a degree of flex-

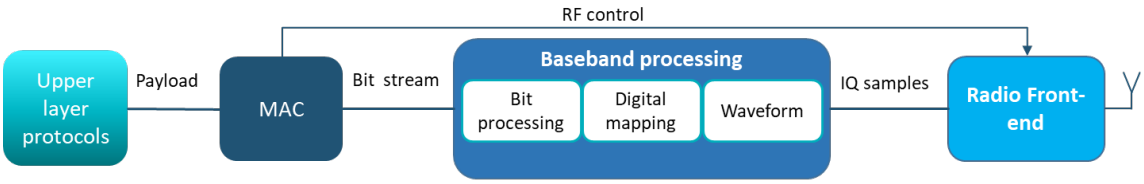

Figure 3:6: RF communications system architecture

ibility that allows the employment of a common PHY in scenarios with contrasting requirements [9].

The PHY connects the data from/to upper communication layers to the physical medium. The next layer up in the communication protocol stack is the

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

medium access control (MAC), which is used to control the access to the shared transmission medium, i.e., it is responsible for allocating and scheduling the resources. As illustrated in Figure 3:6, the PHY can be split into: (i) bit processing responsible for performing scrambling, channel coding and interleaving, (ii) digital mapping, which produces complex-valued symbols by mapping several bits to one symbol, e.g., quadrature amplitude modulation (QAM) mapping, (iii) waveform, which generates discrete-time samples that are adequate for the transmission medium and contain the data symbols. As an example, the Fourier transform of the data symbols is used in orthogonal frequency division multiplexing (OFDM).

3.2.2 INGENIOUS CONTRIBUTION AND INNOVATION

Innovation Summary: Flexible PHY/MAC (UE Side) and Compute Platform

Flexible PHY/MAC (UE side):

- Flexible PHY/MAC FPGA implementation.

Compute Platform:

- Deployment of baseband processing chains on RISC-V cores and utilization of the network-on-chip (NoC) for data transfer between stages

Benefit due to integration of the components:

- The integration of a flexible non-3GPP PHY/MAC with 5G core and MANO allows the realization of industrial and supply chain applications.
- The flexibility enables the development of a custom PHY/MAC in a private network, such as industrial networks.
- Customization or upgrading of communications capabilities for IoT devices
- Possibility to share general-purpose compute cores between applications and baseband processing
- Default isolation between tiles where functions are executed, thus enhancing physical layer security.

The flexibility of the PHY refers to the ability to change the baseband parameters, such as the mapping and channel coding. 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 waveforms, and to create an optimized data representation based on given requirements, hardware constraints, and channel condition. 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 3.1.

Within iNGENIOUS, TU Dresden (TUD) and BI collaborate to port software-implemented PHY processing stages such that they run on the BI compute platform. The computations in the transmitter chain are separated into eight blocks that are executed as programs on RISC-V processor cores in the M^3

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

platform. The modules cooperate in the PHY processing chain by exchanging messages through the NoC. They can distribute the computational load across multiple processing cores, thereby potentially saving energy compared to running on a single high-performance core, while also allowing run-time flexibility. Details of this application-level SDR deployment scenario are described in deliverable **D3.3 Secure, private and more efficient HW solutions for IoT devices** [6]. Note that the transmitter chain running on M³ provides the IQ samples, and a digital-to-analog converter (DAC) and RF front-end must be attached to M³ hardware platform for generating the actual radio signal. This task can be easily accomplished with light weight SDR equipment, such as the USRP mini[1].

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

- Compile-time flexibility for enabling 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.

Alongside the flexible PHY, a flexible MAC is required to convey control information about the employed 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 4.1.

3.2.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

This subsection summarizes potential exploitation plans for the flexible PHY/MAC. The proof-of-concept is demonstrated through the Factory UC.

Component Group: Flexible PHY/MAC (UE Side) and Compute Platform
Relevant for use cases: Factory **Evaluation use case:** Factory **Test cases:** UC1_TC_01, UC1_TC_02, UC1_TC_03 **Exploitation Potential:** • **TUD:** The flexible PHY/MAC allows real-time experiments of new innovations in PHY/MAC design under realistic channel conditions instead of using model-based simulations. • **BI:** Valuable lessons learned and requirements from a real SDR implementation on BI's M³-based compute platform. Insight into what accelerators may be beneficial to make SDR workloads more efficient and yet flexible.

[1] https://www.ettus.com/all-products/usrp-b200mini-i-2/

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

3.3 Component Group: Immersive Devices, AGVs, and 5G Modem

In this section the group of components related to Immersive Devices, 5G NR Modem and AGVs are described. They are divided into two parts, the one that refers to the vehicle itself (AGV) and the one that brings together all the necessary elements to give the driver a remote driving experience with telepresence (MR Cockpit and haptic gloves). The 5G modem is present in both parts, enabling the communication through the 5G network. It is highlighted the innovative contribution, the benefits, the field of exploitation and the use cases of each component.

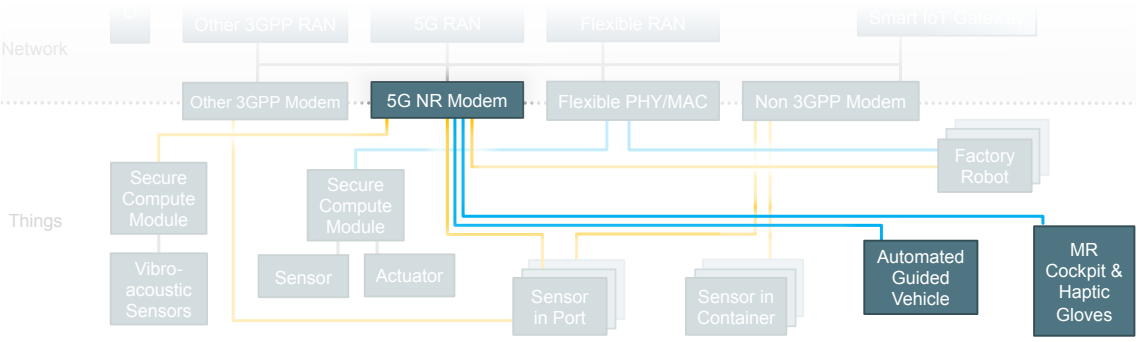

Figure 3:7: Component group consisting of devices for an immersive cockpit, remote-controllable AGV, and 5G modem

3.3.1 STATE OF THE ART BEFORE INGENIOUS

The immersive components currently have their main application center in the field of video games. There are many consoles and computers that include tools to offer an immersive experience in their games, allowing interaction with both people and objects in a virtual world. The scope of the project and the remote driving is closely linked to this field. Although initially games have been developed to allow the user the immersion in a racetrack, this idea can be extrapolated to a real environment in which the driver doesn't have to be physically in the vehicle.

AGVs are being increasingly used in different areas such as factories or farm fields. These systems make it easier for operators to perform certain tasks that can be mechanical and repetitive, which is why they allow human action to be replaced with that of an unmanned vehicle. Nevertheless, AGVs cannot be fully autonomous on unpredictable or dynamic environments, as well as changing situations when the robot reaches its functional limits, when they need to be supervised and/or controlled by human operators. In those situations, typical screen-based teleoperation systems do not provide the stimulation and the spatial perception needed to precisely manipulate the AGVs.

Immersive components such as mixed-reality head-mounted displays (HMDs) and haptic devices solve these issues by adding information and providing a more intuitive control of the AGV. The combination of both concepts allows to extend the actions that an AGV can carry out. Thanks to immersive remote driving, these tasks are carried out more safely and their scope can be extended. However, when the cooperation between humans and robots is

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

performed remotely, latency issues appear that are caused by transmission over a network. If a conventional LTE network is used, the excessive delay on the communication medium affects twice to the total latency, which in mobile robots leads to instability or imprecision, whereas in humans it causes the sensation of discomfort or lack of interaction. The use of low-latency 5G networks to communicate the immersive devices and the AGV is key to avoid these problems, as well as to fulfil the other requirements (mainly throughput and reliability) of remote driving.

3.3.2 INGENIOUS CONTRIBUTION AND INNOVATION

AGVs are used in industry and maritime ports, among other scenarios. In some situations, it is needed that an operator takes control of the AGV for performing a specific task. In the iNGENIOUS project, a technological integration between AGVs and immersive devices is approached for avoiding hazardous situations and improve the safety of the operations. The 5G network is used for enabling the communication thanks to its low-latency specifications and data transmission capabilities. Immersive devices used in the context of the project such as MR glasses and haptic gloves are defined in deliverable **D3.4 Bio-haptic and XR-enabled IoT devices** [10].

Innovation Summary: Immersive Devices, AGVs, and 5G Modem
Mixed reality glasses: • Enhance the driving experience by extending the spatial perception of the user • Create a safer and more intuitive pilotage by displaying a user interface with relevant information about the remote driving • Integration of AGV events and signals in the field view **Haptic gloves:** • Avoid collisions by warning the user about nearby obstacles • Increase the perception of the user by informing about the state of the AGV's route via haptic feedback • Create an intuitive and user-friendly way of controlling the AGV's route (via gestures) **Cameras 120° and other sensors:** • Virtualize the MR 3D visualization delivered to the cockpit's controller • Achieve telepresence of the driver • Enable measurement of the distance to obstacles **AGVs (ASTI's and Robotnik's models):** • The AGVs are connected to the 5G network and provisioned with cameras and sensors • Can be controlled from a cockpit situated far away with haptic remote control Exposure of internal signals and variables by ASTI AGVs and low-latency event communication • Automatic and manual mode supervision of ASTI AGVs **5G modems:**

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

- Enable the achievement of stringent throughput, latency, and reliability requirements. Information about the values can be found in deliverable **D2.2 System and architecture integration (Initial) [1]**.
- **The 5CMM modem** enables machines to connect to the 5G network in a compact and widely configurable and versatile way. It can be connected to any machine with an easy plug & play. This modem will be used in Factory and AGV use cases.
- **Another 5G modem** will be employed in the AGV demos. This modem works in mmWave, it is from the manufacturer Askey, and will be provided by NOK.

Benefit due to integration of the components:

- With the combination of 5G networks, cameras and MR glasses, the remote pilot has a sense of presence in the vehicle. This improves the driving experience and increases the accuracy of the control.
- The integration of the haptic gloves in the immersive cockpit enables new natural and intuitive ways of controlling or driving the AGVs, enhancing the versatility of the solution.
- Using the modems with any of the other components allows them to wirelessly communicate between them through the 5G network, which has benefits in mobility, latency, reliability, and throughput.
- With all the immersive devices the safety and work quality of machine operators in supply chain will be improved, since they will be able to work from indoors.

Immersive components such as mixed-reality and haptic devices allow to minimize conflict or facilitate the understanding between humans and AGVs. On the one hand, mixed-reality HMDs facilitate remote driving by providing detailed user interfaces and extended spatial perception. On the other hand, haptic feedback enabled by haptic devices such as vibrotactile are useful for avoiding collisions or receiving information about the AGV's state.

In iNGENIOUS, immersive devices will be used to enhance the safety conditions of workers. They will enable the remote control of the AGVs in real-time. For connecting to the 5G network, 5G modems are used both in the AGV and in the cockpit that includes all the immersive devices.

The 5G modem used in the project is shown in **Fehler! Verweisquelle konnte nicht gefunden werden.**. It is innovative, because as a plug & play component, it can be easily connected to all kinds of devices using the integrated Ethernet port. It is also possible to configure it through a software, making it versatile and useful for all kinds of use cases and situations. In terms of hardware, it is also possible to configure the number and types of antennas. The size of the modem is compact compared to other commercial modems. For a better description of the modem see **Section 3.7** of deliverable **D2.2 System and architecture integration (Initial)** [1].

Figure 3:8: 5CMM's 5G modem

For the integration of the immersive devices in a cockpit, an application has been developed (Figure 3:9). In this cockpit application it is possible to see

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

what the AGV sees in an immersive way using the MR glasses. The control of the AGV is also in the same application, using the haptic gloves or a steering wheel and pedals. Further explanation can be found in **D3.4 Bio-haptic and XR-enabled IoT devices** [10].

Figure 3:9: MR glasses and haptic gloves used with a cockpit application

3.3.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

This group of components mainly covers the AGV use case, although the integration between the AGV and the 5G modem will also be performed in the Factory use case. Exploitation will focus on the commercialization of the components and as an integrated service. Further information about exploitation is available in **D7.3 Final dissemination, standardisation and exploitation** [3].

Component Group: Immersive Devices, AGVs, and 5G Modem
Relevant for use cases: AGV **Evaluation use case:** AGV **Test cases:** UC2_TC_01, UC2_TC_02, UC2_TC_03, UC2_TC_04 **Exploitation Potential:** • **5CMM's 5G modem** has a clear exploitation route. The modem will be commercialized as a compact and configurable device for enabling 5G in any object. **5CMM's cockpit** is a solution for remote and autonomous driving using immersive devices such as MR glasses, haptic gloves, pedals, wheels, controllers, and keyboards among other devices all integrated in just one cockpit. This solution will be exploited in the market as an autonomous and remote driving solution for factories and maritime ports or terminals. • **NOK's components** will be needed in current and future generations of **autonomous AGVs**. The **mixed reality** glasses combined with the **cameras** and other **sensors** are a solution to achieve the telepresence, giving the driver of a vehicle the sense to be inside of it. This technology has a clear use in the field of remote driving of different vehicles in several real scenarios. In relation to **5G modems**, they have wide variety of uses in any field of daily life

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

or more complex applications. They allow any device with a 5G connection for the communications with other devices.

- **ASTI** will exploit remote monitoring and driving across its entire AGV portfolio. However, the application of this function seems to be a priority on its outdoor AGVs, as they are subject to hazardous conditions and share the workspace with all types of vehicles.
- **Haptic gloves** like those developed by former consortium partner NED include novel hardware and software solutions that can be exploited in many verticals, such as healthcare, education, entertainment, industry and logistics. Regarding AGV control, they can be commercialized either integrated into 5CMM's cockpit or as an independent device, depending on the desired functionalities of the application. Their biggest potential, however, consist in controlling robotic arms that mimic the behaviour of human arms.

3.4 Other Components

In **D2.2 System and architecture integration (Initial)** [1], we describe two additional components of the things layer within the iNGENIOUS architecture as shown in Figure 3:10.

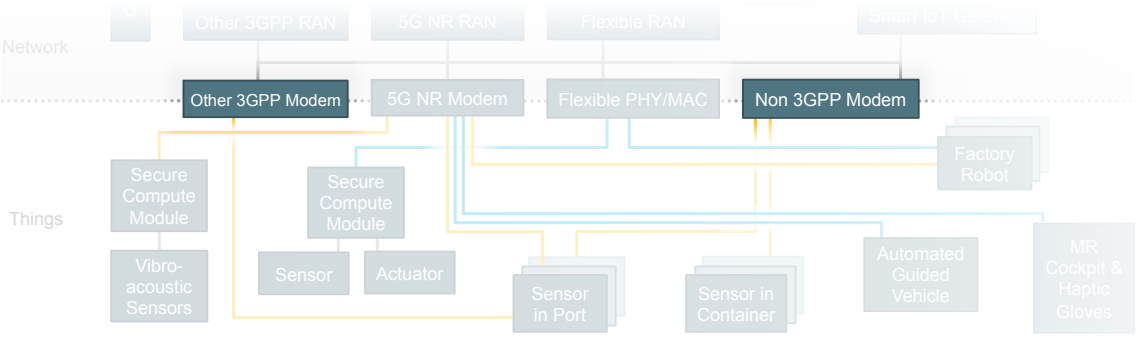

Figure 3:10: Other connectivity components in iNGENIOUS things layer

In **Section 3.6** of the D2.2 deliverable, we summarize what the iNGENIOUS consortium investigates in terms of new innovative air interface solutions for *Cellular IoT Connectivity*. This activity is in line with improvements discussed in the 3GPP standardization body.

In **Section 3.6** of D2.2, *Non-cellular IoT Connectivity* is described. No new functionality is developed by the iNGENIOUS partners in this area. However, the existing non-cellular IoT connectivity solutions such as modems are critical to support the project's use cases and therefore reused as important parts of the iNGENIOUS architecture. We list both components here but refer the reader to **Sections 3.6** and **3.7** of deliverable **D2.2 System and architecture integration (Initial)** [1] for an overview. Additionally, for Cellular IoT connectivity, a detailed discussion of iNGENIOUS innovations can be found in deliverable **D3.2 Proposals for next generation of connected IoT modules** [11].

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.

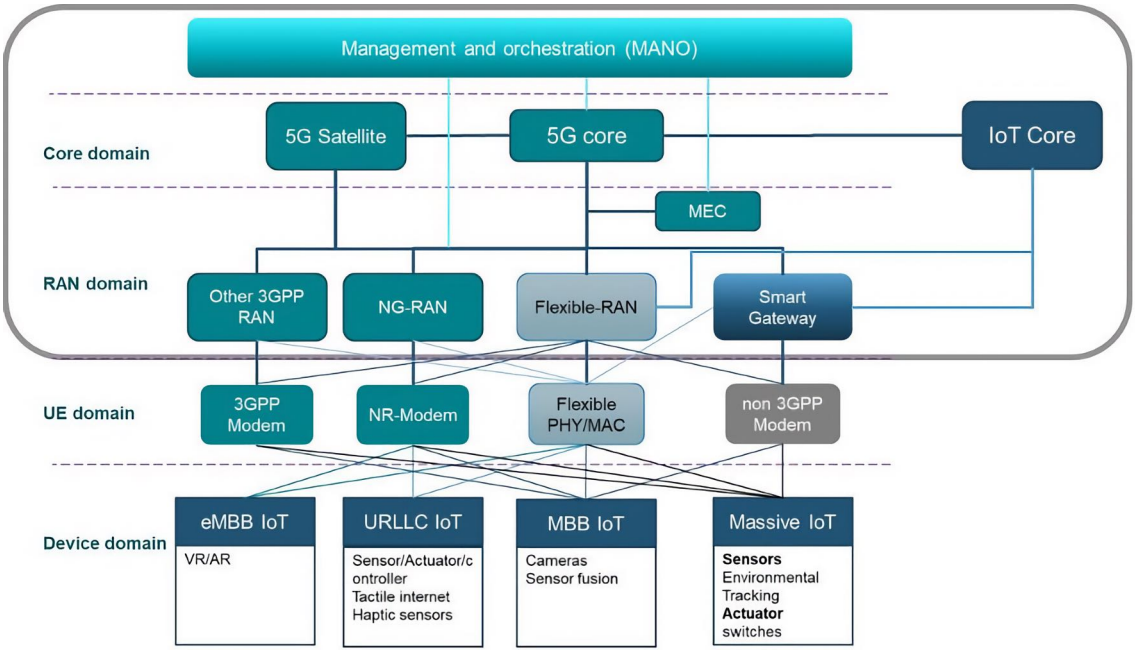

Figure 4:1: iNGENIOUS network architecture

Figure 4:1 visualizes the physical and logical network components and how they interact with each other. In the iNGENIOUS cross-layer architecture, these components are part of the network layer (Core and RAN domain) and things layers (UE and devices). In this chapter, the focus is on the interaction of components located in the Core domain, the radio access networks (RAN) domain, and management and orchestration (MANO), as highlighted in Figure 4:1. A summary of relevant radio access technologies (RATs) is provided at the beginning of **Chapter 4** in deliverable **D2.2 System and architecture integration (Initial)** [1]. In the following Section 4.1, we focus on the component group that contains key 5G technologies, which aim at converging all types of IoT communication in one network. Additionally, we describe integrations of the iNGENIOUS Smart IoT Gateway and satellite connectivity in Section 4.2.

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

4.1 Component Group: 5G Core, 5G RAN, Flexible RAN, and MANO

Figure 4:2 depicts the iNGENIOUS IoT network layer components which realize the 5G network functionalities. These are the 5G Core (5GC), 5G RAN, Flexible RAN innovating PHY/MAC, and Management and Orchestration (MANO). While the 5GC, 5G NR and Flexible PHY/MAC are integrated to provide 5G communications in support of the different iNGENIOUS Use Cases, the MANO component provides those overarching network and service orchestration capabilities that allow facilitating the end-to-end 5G network integration and provisioning of added value services and network slices.

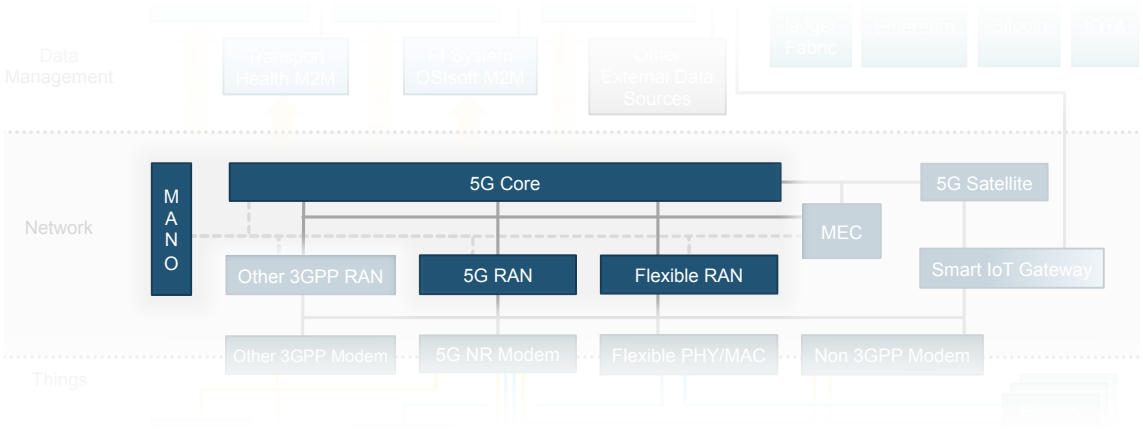

Figure 4:2: Main 5G Network components within the iNGENIOUS network layer

4.1.1 STATE OF THE ART BEFORE INGENIOUS

5G technology is the order of the day for different tasks, both daily and complex. This is the new generation of mobile networks that provides the ability to obtain very low latency connections, giving rise to the use of applications that require the exchange of data in real time.

The capabilities provided by this type of network mean that efforts are currently being made to develop cores that allow the connection of many devices that exchange information in real time. Some different examples can be found in the real time applications to reduce road accidents; or life-saving applications that can take flight thanks to lag-free guaranteed connections; or production lines so predictive they can prevent interruptions well before they occur.

Closer to the scope of the project, in the field of remote and autonomous driving, the use of this type of network that allows fluid communication in real time to minimize possible accidents is essential. A more detail explanation about this kind of network and specific state of the art can be found in deliverable **D3.1 Limitations and improvement axis for the communication of IoT devices** [5].

The 5G-related 3GPP standards also define the PHY/MAC layers. However, the flexibility with regard to parameters such as MCS, the discrete Fourier transform (DFT) size, and precoding is limited, because only pre-defined configurations can be selected. A more general solution is to optimize the user's signaling is by changing the channel encoding and waveform, and to flexibly

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

provide multiple access schemes, which is the goal of the flexible PHY/MAC implementation.

Regarding the research prototyping activities, the existing SDR-based radio implementation developed by TUD in previous European projects such as ORCA [12], focused on the PHY without dynamic resource allocation, i.e., single UE with a fixed configuration. In addition, it was not integrated with an end-to-end 5G network, with only standalone PHY/MAC experiments and demonstrations with the prototyped devices were possible.

To manage and automatically configure 5G network resources, including network and computing across end-to-end 5G infrastructures, 3GPP proposes an architecture for Management and Orchestration (MANO) of network slices [13]. Current MANO framework solutions still mostly rely on static and ossified management procedures, and do not yet provide flexible coordination and operation logics capable to satisfy changing network and service conditions, especially when it comes to integrate 5G NR, NG-IoT, and edge computing in support of supply chain and industry 4.0 services. Moreover, the full automation of network slice orchestration and runtime operation, with the integration and adoption of AI/ML technologies is still in its early stage. In this context, a deeper gap analysis study about the SOA is available in **Section 4.1.3** of deliverable **D4.1 Multi-technologies network for IoT** [14].

4.1.2 INGENIOUS CONTRIBUTION AND INNOVATION

Innovation Summary: 5G Core, 5G RAN, Flexible RAN, and MANO

5G RAN, 5G Core:

- Build upon existing, standardized 5G innovations:
  - Enhanced mobile broadband (eMBB)
  - Ultra-reliable low latency communications (URLLC)
  - Massive machine type communications (mMTC)
- Simultaneous connections interfacing the 5G Core and the MEC
- Application Function to request multiple flows with different QoS

Flexible RAN:

- Smart flexible RAN integrated to MANO and 5G Core
- Dynamic resource allocation

MANO:

- Fully automated and AI enabled network slice management, orchestration and runtime operation

Benefit due to integration of the components:

- Increased flexibility of management and orchestration framework
- Slicing capabilities in 5G, 5G NR and Flexible RAN

The 5GC architecture compared to previous generations is designed to support machine, UE and IoT communications. For this reason, Network Slicing was introduced to create virtual instances of the core to separate traffic with different high-level requirements. For instance, IoT data flow can be isolated from consumer data flow, each one of them belonging to different 5G slices.

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

Network Slicing: In iNGENIOUS, Cumucore (CMC) developed a 5GC solution with network slicing capabilities that support traffic segregation for different service requirements. 3GPP has defined a set of standard slices to address the needs of different applications based on the traffic type such as Enhanced mobile broadband (eMBB), Ultra-reliable low latency communications (URLLC) and massive machine type communications (mMTC). The CMC 5GC integrates the network slice management functionalities that are specified by 3GPP, and allow to set up multiple slices across RAN, Edge, and Core Network domains. Specifically, a dedicated network function within the CMC 5GC implements the Network Slice Management Function (NSMF) capabilities exposing dedicated APIs towards the iNGENIOUS MANO framework to enable automated and dynamic setup and configuration of slices (see Figure 4:3).

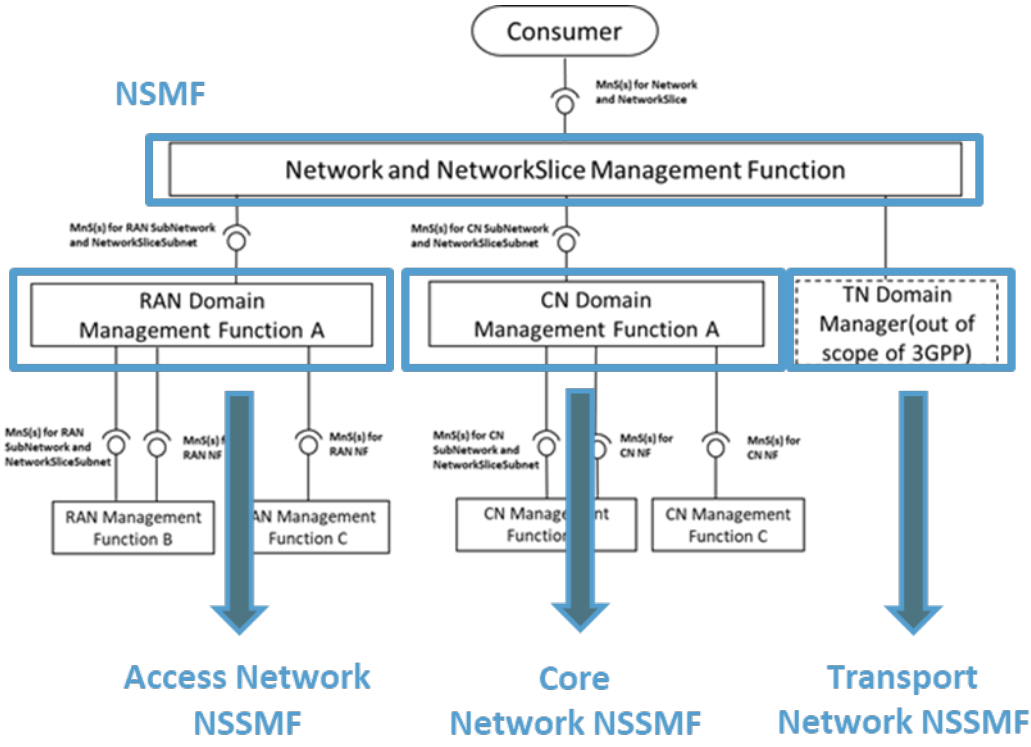

Figure 4:3: 3GPP Network slice management architecture [15]

Moreover, 3GPP has introduced new 5GC network functions to increase flexibility and scalability. Indeed, the CMC 5GC architecture also includes network functions that collect data from other network functions for monitoring. This information is made available to external orchestrators to take some corrective actions. Specifically, the Network Data Analytics Function (NWDAF) represents operator managed network analytics logical function. The NWDAF provides interface to the iNGENIOUS MANO framework to monitor the 5G system to trigger some scalability policies such as spawning new network functions (i.e., UPF to increase capacity).

Flexible RAN: At the RAN side, to support a diverse range of mobile applications, a variety of PHY/MAC configurations are required to be supported. As discussed in Section 0, the UEs can also be equipped with flexible PHY/MAC, which allows a customizable RAN. This architecture supports different configurations, where 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

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

the required standard interfaces, as shown in Figure 4:4. The interface agreement on how the devices should exchange data among themselves and with an industrial application developer is exemplified in the Factory use case, and further details are presented in Section 6.1. The flexible PHY/MAC aims at allowing the selection of the best configuration based on the channel status and application requirements.

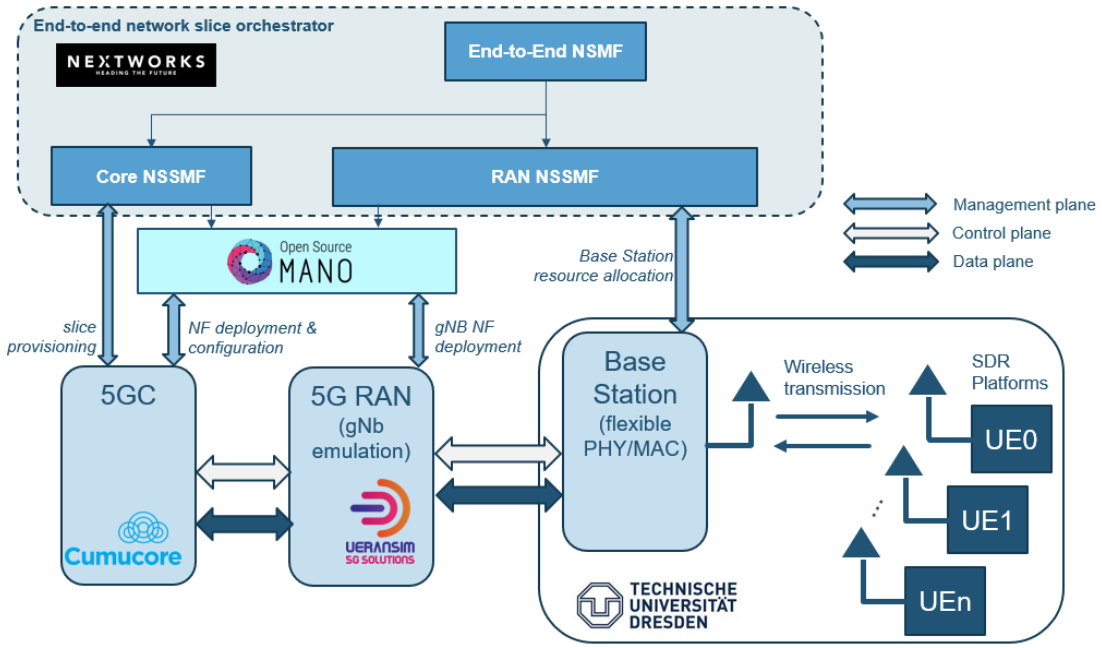

Figure 4:4: Flexible RAN architecture

In iNGENIOUS, TUD's PHY implementation has been improved, since a multiple access scheme has been implemented to allow dynamic resource allocation. In order to achieve this, a simple control channel has been developed. It allows the base station to have control over the radio resources, and to dynamically set the user's configurations to target the application needs. The implemented flexible MAC design includes the multiple access schemes based on time-division multiple access (TDMA), but in general other schemes such as frequency-division multiple access (FDMA), space-division multiple access (SDMA), code-division multiple access (CDMA), and any combination of them are possible. 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.

Moreover, an integration of this PHY/MAC solution with the 5G network has been performed to enable 5G connectivity to the different UEs, and validate the PHY/MAC approach in a realistic 5G enabled industrial scenario. This has been done by integrating the PHY/MAC resource allocation with the 5GC and the iNGENIOUS MANO framework to setup and configure specialized end-to-end network slices tailored to the various mobile applications and UE requirements. Moreover, in this context, the integration of AI/ML techniques within the MANO framework (as described below) can help in achieving smarter NR networking and resource allocation at runtime.

MANO: The combination of 5GC and RAN technologies towards the realization of end-to-end 5G networks guarantees to satisfy the requirements of mMTC,

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

URLLC and eMBB services and slices. Still, there is the need of augmenting the 5G network technologies with network management and orchestration functionalities to enable heterogeneous and concurrent services (such as those deriving from supply chain, maritime ports and industrial use cases) to coexist on top of shared 5G end-to-end infrastructure. Here, from communication and network perspective, different requirements in terms of latency, bandwidth and so on must be satisfied. In this context, the iNGENIOUS MANO framework allows to provision, configure, and operate heterogeneous and concurrent type of end-to-end network slices (mMTC, URLLC and eMBB), coordinating the allocation of network and computing resources across various domains, including radio, edge and core. This allows to provision separated logical networks on top of the same physical infrastructure, tailored to specific service requirements.

As anticipated above, the iNGENIOUS MANO framework is a key enabler for the integration of 5GC and RAN technologies, and specifically the automated deployment, management, and coordination of heterogenous services and slices. Indeed, it has been designed and prototyped to interact with other components in the iNGENIOUS IoT network layer, to provide the required management and orchestration functionalities as depicted Figure 4:5.

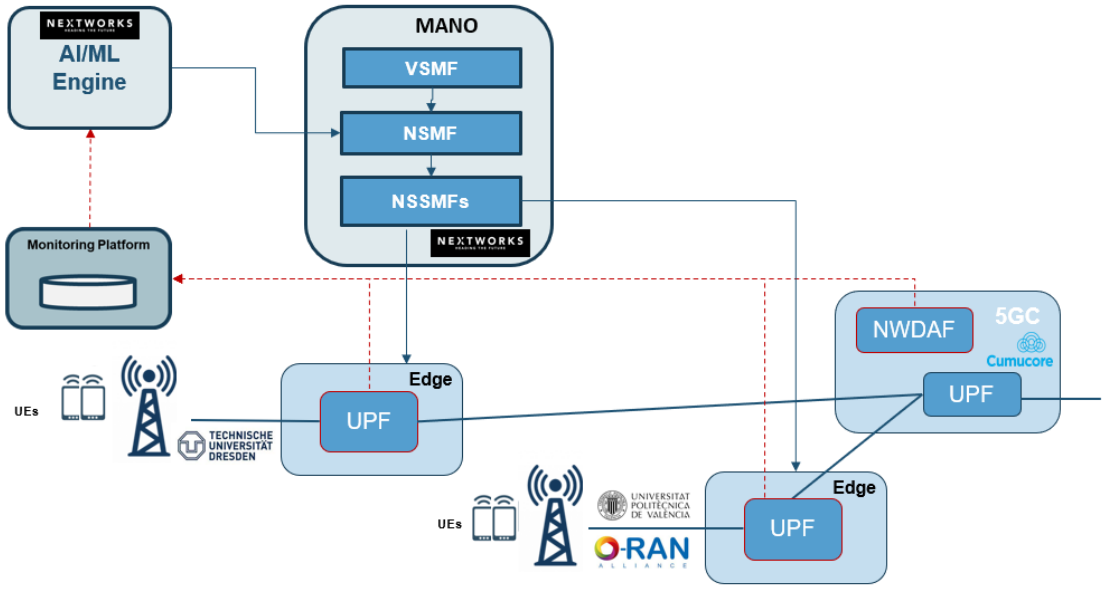

Figure 4:5: Main interaction between MANO and network layer components

The designed and prototyped MANO framework, which extends and enhances the Nextworks slicer software tool, allows to coordinate the network and compute resource allocation across the various domains by means of dedicated network slice subnet management functions (NSSMFs). Each NSSMF is dedicated to the management of per-domain network and compute resources (e.g., RAN, edge or core), exposing common APIs and operations towards the end-to-end network slice management function (NSMF) which glues together the various domains and subnet slices in support of tailored end-to-end network slices. On top of them, a vertical service management function (VSMF) provides end-to-end service coordination logics to map supply chain and industrial service requirements and applications with underlying network slices. This approach assures to have a common orchestration and operation logic which can be easily adapted depending on the specific

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

RAN, edge and core technology used. In addition, the iNGENIOUS MANO framework is providing full automation in network slice operation by integrating with an AI/ML engine that applies tailored AI algorithms to optimize the network slices at runtime. Specifically, this is enabled by a monitoring platform integrated with the MANO. It allows to collect slice and network functions performance data and allowed to implement a specific AI algorithm for triggering predictive network slice and UPF scaling actions. The aim is to prevent network slice performance degradations caused by UPF congestion. In summary, the iNGENIOUS MANO framework integrates and interacts with the following IoT network layer components:

- The CMC 5GC, managing and orchestrating network slices where traffic coming from different UEs is served
- The TUD flexible PHY/MAC, enabling integration with the 5G network (and 5GC), providing slicing capabilities across the end-to-end network

More details about the software design and implementation of orchestration framework and the related AI/ML integrated approach can be found in the **Section 4** of deliverable **D4.4 Service orchestration at the edge** [16].

4.1.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

Component Group: 5G Core, 5G RAN, Flexible RAN, and MANO

Relevant for use cases: Factory

Evaluation use case: Factory

Test cases: UC1_TC_04, UC1_TC_05, UC1_TC_06, UC1_TC_07, UC1_TC_08, UC1_TC_09, UC1_TC_10, UC1_TC_11, UC1_TC_12, UC1_TC_13

Exploitation Potential:

- **CMC:** Development of commercial version of 5G Core including network slice manager to create and allocate different network slices to different groups of users each with different profile. CMC also has implemented the NWDAF with an interface that allows an external orchestrator for scalability management. An application function (AF) is implemented to allow request of multiple flows with ongoing session to allow multiple data stream with different QoS.
- **NXW:** The software prototype of the MANO framework with AI/ML capabilities for assisted end-to-end network slice orchestration and operation will provide Nextworks the opportunity to exploit this 3GPP compliant framework for 5G nonpublic network deployments. Specifically, this is aligned with the company interest and target towards the industry 4.0 market. In this context, the integration, validation, and demos carried out in the Factory use case, where Nextworks is also providing and integrating its 5G network monitoring data collection framework, are key to assess these capabilities and early validate the readiness of the developed MANO framework for pre-commercial pilots.
- **TUD:** Flexible PHY/MAC implementation in SDR and its integration with 5G compliant core and MANO allows for a unique testing platform where the interaction and coexistence of non-3GPP radio access technologies can be investigated, and further developed in the context of heterogeneous industrial networks.

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

4.2 Component Group: Smart IoT Gateway and Satellite

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.

Therefore, the Smart IoT Gateway gathers and processes the data from the heterogeneous IoT devices and sends the data to IoT Cloud through satellite backhaul or terrestrial network.

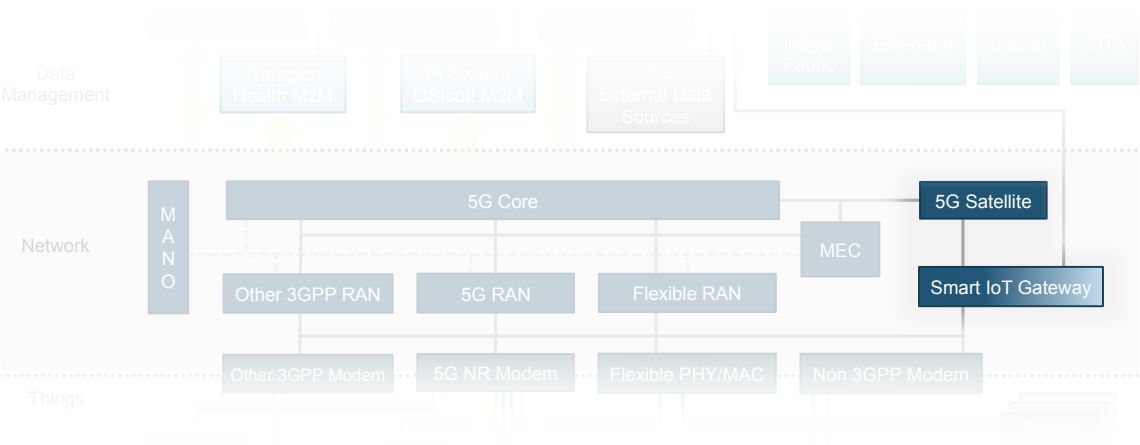

Figure 4:6: Component group consisting of satellite and smart IoT gateway

4.2.1 STATE OF THE ART BEFORE INGENIOUS

Smart IoT GW: When collecting data from heterogeneous IoT devices via a single unified gateway device, a self-developed solution was the only available option. Since there was no strictly defined standard for physical and link layer protocols to be used for IoT devices, the Smart IoT GW builds on present de-facto standards to provide a unified gateway for IoT communication. It is easily extendable due to its open and modular architecture, allowing for straightforward integration with different (IoT) communication standards, like ZigBee, Modbus or even serial connections.

Usually, sensor and monitoring data is immediately sent to a cloud server for post-processing and data analytics. With its edge-/fog-computing capabilities, the Smart IoT GW enables data analytics “on the edge” and allows for context-specific processing of the sensor data – e.g., prioritization of specific transmissions. Furthermore, it lays the foundations to introduce AI and machine learning closer to the source of the information for more specific predictions and handling of certain events, based on the individual use case.

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.

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

The satellite backhaul solution is well used in practice. Satellite backhaul serves indirect satellite access use cases, where the satellite network is used to transport and optimize traffic between IoT devices and core networks. 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 such as the SES Smart IoT Gateway
- Have low CAPEX set-up costs costs, e.g.
    - no additional terrestrial infrastructure required
    - can leverage low-cost satellite terminals
- 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. Within the Transport and Ship use cases 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.

Typically, a satellite remote deployment requires the installation of a satellite VSAT antenna and remote terminal to meet the link budget requirements for end-to-end connectivity. Direct access for IoT devices brings a new set of challenges where it is not practical to install a VSAT antenna to connect each individual IoT device. Therefore, a Direct-To-Satellite IoT solution needs to consider working in an environment with a reduced signal-to-noise ratio (SNR) and link-budget considerations. Direct-To-Satellite IoT remote terminal cost and footprint requirements are also a major factor.

4.2.2 INGENIOUS CONTRIBUTION AND INNOVATION

The main innovations of the Smart IoT GW and satellite networking are summarized in the following table and paragraphs.

Innovation Summary: Smart IoT Gateway and Satellite
Smart IoT Gateway: • Support of different IoT protocols • Message prioritization • Detection, monitoring, and reporting on availability of backhaul connectivity **Satellite:**

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

- Investigation of direct access over satellite for IoT devices

Benefit due to integration of the components:

- Traffic optimized for satellite communications
- IoT connectivity in areas where terrestrial networks cannot be used

Smart IoT Gateway: Taking the OSI model as a reference, the Smart IoT GW exposes 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^2C, or SPI) as shown in Figure 4:7. The Smart IoT GW is smart enough to manage the routing and direct the received messages to the right output interface in the right timing. Several factors have been 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.

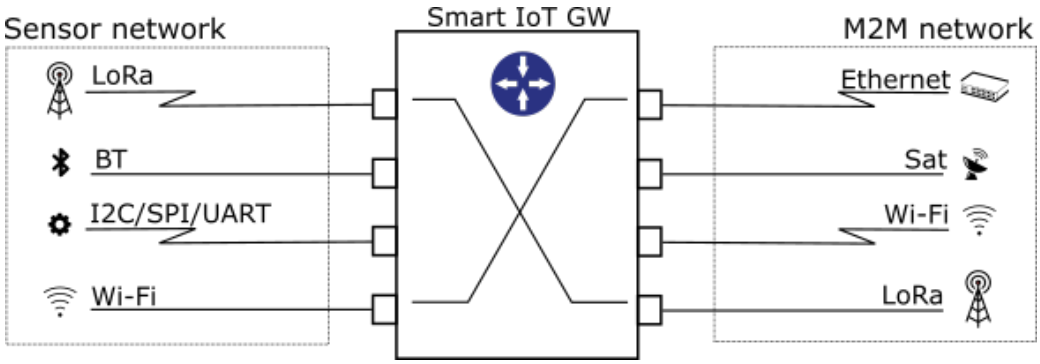

Figure 4:7: Smart IoT GW PHY interfacing

Direct Access: As mentioned earlier in the state of the art, unlike the satellite backhaul solution, direct access is where IoT devices are connected directly to the satellite network. ST Engineering iDirect investigated the enhancement of existing proprietary satellite waveforms to support the direct access over satellite use case.

The investigation included:

- An analysis of the current state of the art of Direct-To-Satellite IoT

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

- An analysis of the link budget requirements of a Direct-To-Satellite IoT solution
- Identifying the changes and enhancements required to update existing satellite communication systems to support Direct-To-Satellite IoT solution
- Proof-of-concept of a Direct-To-Satellite IoT implementation based on existing ST Engineering iDirect technology

4.2.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

This subsection summarizes potential exploitation plans for the Smart IoT Gateway and Satellite technologies, which have been demonstrated through the Transport and Ship use cases. More information about the exploitation plan can be found in the iNGENIOUS deliverable **D7.3 Final dissemination, standardisation and exploitation** [3].

Component Group: Smart IoT Gateway and Satellite
Relevant for use cases: Transport, Ship **Evaluation use case:** Transport, Ship **Test cases:** UC3_TC_17, UC3_TC_18, UC3_TC_19, UC3_TC_21, UC3_TC_22, UC3_TC_23, UC4_TC_08, UC4_TC_09, UC4_TC_10, UC4_TC_11, UC4_TC_12, UC4_TC_13, UC4_TC_14, UC4_TC_15, UC4_TC_16, UC4_TC_17, UC4_TC_18, UC4_TC_19, UC4_TC_20 **Exploitation Potential:** • **SES:** SES will leverage the iNGENIOUS developments in the Smart IoT GW to increase and customise SES service offering for commercially attractive mMTC use cases and for multiple market verticals, such as Fixed Data, Aero, Maritime, Energy, Government, Cloud, and Video. • **iDR:** iDR will leverage the iNGENIOUS findings to further research and develop standards based and proprietary use cases for indirect and direct access to IoT devices over a satellite network. iDirect will target commercialization of project findings and outcomes to improve their IoT product and service offering. • **FV** and **COSSP:** The container tracking is an essential part of the supply chain and logistics to make them more efficient. By monitoring and tracking seamlessly the container in near real-time, it allows to provide all the supply chain players and stakeholders a full traceability and to optimize the transport and the storage of containerized goods. Any event related to a container is quickly notified and is allowing efficient analytics as well as taking related decision such as new sourcing plans if needed.

4.3 Other Components

In **Section 4.8** of **D2.2 System and architecture integration (Initial)** [4], we describe one additional critical building block in the network layer of the iNGENIOUS architecture: *5G Security*. No new security features are developed by the iNGENIOUS partners, but the existing 5G security features within all 5G network components are critical to support the project's use cases. For a summary, we refer the reader to the respective section of D2.2.

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

5 Data Management Layer

On top of the IoT things and network layers, iNGENIOUS proposes an interoperability layer with data management capabilities that is able to collect data from multiple data sources. This layer interoperates with different M2M platforms, including legacy systems such as Port Community Systems (PCSs). Furthermore, it interoperates with DLTs to address data security, data immutability, and data privacy aspects.

Data Virtualization Layer: iNGENIOUS exploits the use of different M2M platforms, which are adopted 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 component based on the Data Virtualization approach. This component, the Data Virtualization Layer (DVL), acts as a federated and interoperable IoT layer for different M2M platforms and external data sources by providing shared access, management, reading, and writing capabilities to different entities (e.g., TrustOS, AI-based platform, maritime events and truck-tracking dashboards). Moreover, it covers security and privacy aspects following a role-based approach and applying pseudonymization techniques to sensitive data sets (e.g., truck plate numbers). 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.

Cross-DLT Layer: 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.

Once data have been collected, processed, and aggregated by DVL according to defined data models, the Cross-DLT layer ensures secure supply-chain event management by recording events as TrustPoints in different DLTs. It allows end users to exploit native DLT capabilities for securing their own data (e.g., data existence proofs and data immutability).

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

Interoperability as a Use-Case Enabler: The iNGENIOUS interoperability layer (based on both DVL and the Cross-DLT layer) is validated by means of three use cases within the project, namely the Port Entrance, Ship, and DVL/DLT use cases. 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. Figure 5:1 provides a high-level view of the interoperability layer. Its components are at the heart of the DVL/DLT use case, which aims to augment the other iNGENIOUS use cases (shown at the bottom of the picture) in terms of data access and management. The following sections of this chapter describe

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

how the different components of the interoperability layer interact with each other.

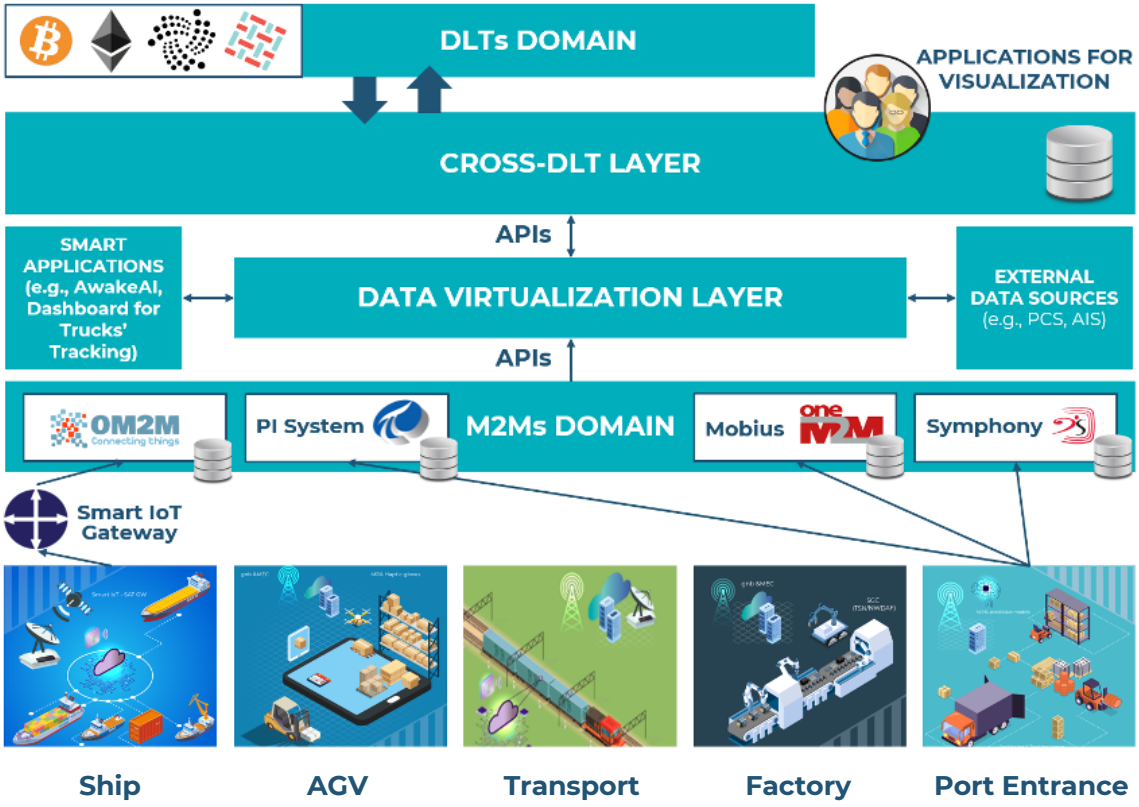

Figure 5:1: High-level view of the interoperability layer enabling the DVL/DLT use case

5.1 Component Group: M2M Platforms and DVL

In this section, we describe and contextualize the Data Virtualization Layer (DVL) as one of two main components of the Interoperability Layer for M2M platform federation as well as for data aggregation.

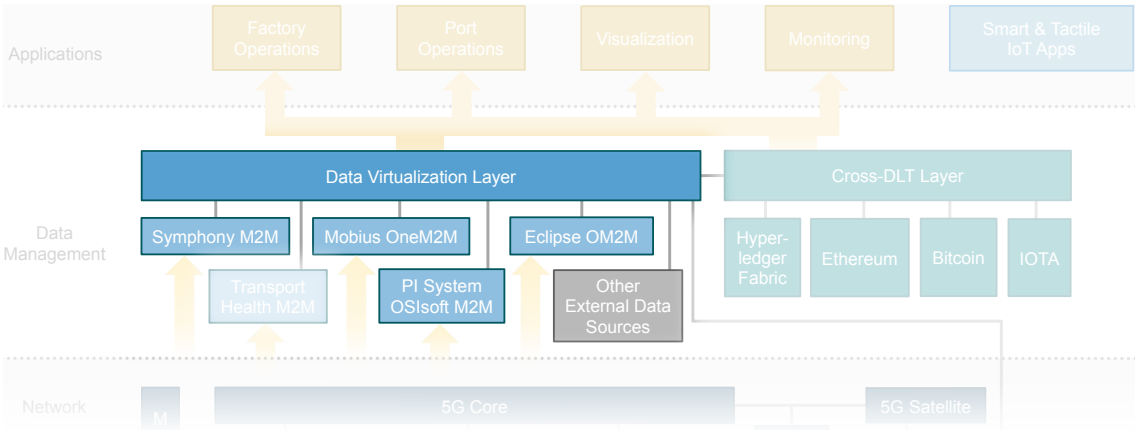

Figure 5:2: Component group consisting of Data Virtualization Layer, M2M platforms and additional external data sources

5.1.1 STATE OF THE ART BEFORE INGENIOUS

In the maritime domain, M2M platforms are part of the existing ICT infrastructure to collect, process, and store raw data coming from the underlying smart devices. Although such platforms are well-suited for different application fields, their interoperability is still limited to the specific use case and/or end user applications. Data are collected and stored by the platform according to its own policies and rules and then exploited by a single application (e.g., visualization). This kind of approach has the limitation that the end user application depends on the underlying M2M platform. This direct dependency makes it expensive to easily perform data fusion and/or data aggregation operations without additional development and integration activities on the back-end side. Moreover, combining different data sets may require the development of custom interfaces, causing additional costs including those related to maintenance and long-term support, as already described in **Section 2** of deliverable **D5.1 Key Technologies for IoT data management benchmark** [4]. As a result of such limitations, business strategies and decisions are not based on all of the available data, which can lead to flawed decision-making.

5.1.2 INGENIOUS CONTRIBUTION AND INNOVATION

Innovation Summary: M2M Platforms and DVL

Data Virtualization Layer (DVL):

- Abstraction of the complexity of the underlying data sources (e.g., M2M platforms and PCS) by implementing a common layer for data access and aggregation
- Adoption of standard interfaces for data access and data consumption (e.g., RESTful interfaces over OData protocol)
- Definition of access roles for data consumers (e.g., TrustOS)
- Support of pseudonymization techniques for personal data based on the data owners' needs, according to GDPR requirements (e.g., HWK, FPE, SHA2 with seed)

M2M Platforms:

- *No relevant innovation is expected in M2M platforms. Instead, iNGENIOUS partners rely on the current state-of-the-art of such technologies, but development of REST API methods to enable the exchange of data with the DVL are needed in some cases.*

Benefit due to integration of the components:

- Technological lock-in avoidance and increased scalability (system performances are not affected by the number of the underlying data sources)
- Alternative approach for the interoperability (based on platforms federation) across standard and non-standard IoT platforms operating in heterogeneous domains
- Data integration costs breakdown and the capability to quickly validate new business models

In iNGENIOUS, the idea is to rely on the DVL as an intermediate component between the underlying data sources (e.g., M2M platforms) and applications by abstracting their complexity and allowing to overcome interoperability limitations. On one side, the DVL allows to easily manage the access to data

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

gathered by every single M2M platform. This is achieved through standard wrappers and connectors for the interaction so that no further developments are required at the application level. On the other side, it allows external applications to easily consume aggregated data, based on defined needs and requirements, by integrating and providing standard interfaces for the communication.

The description of the IoT/M2M platforms that we rely on for the validation of the DVL component is already provided in deliverables **D2.2 System and architecture integration (Initial)** [1] and **D5.2 Baseline iNGENIOUS data management framework** [17]. Here we focus on the way in which all considered components interact and cooperate with each other by briefly describing their configuration. The DVL is part of the DVL/DLT, Port Entrance and Ship use cases and operates under four different scenarios, which are described below.

Scenario 1: This scenario is linked to the DVL/DLT use case where both Port of Livorno and Port of Valencia are involved. Here, the DVL is responsible for providing GateIn, GateOut, Vessel-Arrival and Vessel-Departure events for both seaports. In this case, TrustOS, which is part of the Cross-DLT layer described in Section 5.2 of this deliverable, plays the role of data consumer of such events. Each event is defined by a given set of attributes according to a common data model from Tradelens platform[2], which DVL retrieves from the underlying and available data sources by aggregating available data sets. The structure of these events has been already described in deliverable **D6.2 PoC development, platform and test-bed integration** [18] along with further details. GateIn, GateOut, Vessel-Arrival and Vessel-Departure events for the Port of Livorno are obtained by aggregating data from the Port Community System (TPCS), whereas for the Port of Valencia, only GateIn and GateOut events are considered and retrieved from the PI System OSIsoft M2M platform. In both cases, DVL implements two different connectors/wrappers to interact with both the PCS and the underlying M2M platform. RESTful interfaces are then exposed so that TrustOS can consume such events by associating a TrustPoint and store it across available DLTs. The overall architecture for this

[2] https://platform-sandbox.tradelens.com/documentation/swagger/?urls.primaryName=Event%20Publish%20API

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

scenario is depicted in Figure 5:3 (the Bridge component is part of the Cross-DLT layer and will be further explained in Section 5.2).

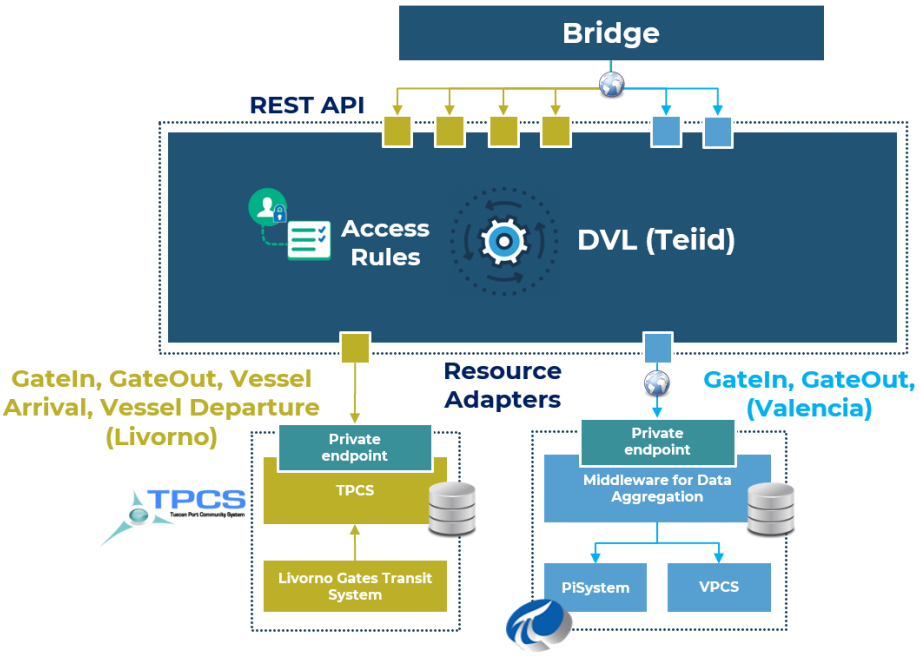

Figure 5:3: Data Virtualization Layer, Scenario 1 architecture

Scenario 2: This scenario is linked to the Ship use case where the Port of Valencia is involved. The DVL is responsible here for interacting with Eclipse OM2M platform in order to retrieve data coming from smart sensors installed on the transported container. In this case the main aim is to detect when the doors of the packed container are closed and the seal is affixed. This information is retrieved from the M2M platform by means of a RESTful connector/wrapper, processed by the DVL, and exposed through a consumable RESTful API. As in the Scenario 1, TrustOS can use such an API to retrieve the event, create a TrustPoint, and distribute it across available set of DLTs for secure storage. Technical details about the architecture for this scenario can be found in deliverable **D6.2 PoC development, platform and test-bed integration** [18].

Scenario 3: This scenario is linked to Port Entrance use case where both Port of Valencia and Port of Livorno are involved. The DVL is responsible for interacting with the Symphony M2M platform in order to retrieve GPS data coming from tracking devices installed on trucks in the Livorno seaport. The device sends data to the M2M platform for storage. This information is then retrieved by the DVL through a RESTful connector/wrapper which allows to directly interact with the platform. Finally, a dashboard-based application can consume the tracking data by invoking a RESTful API at DVL level. The data are then visualized through a dashboard in real time. Technical details about the architecture for this scenario can be found in deliverable **D6.2 PoC development, platform and test-bed integration** [18].

Scenario 4: This scenario is also related to Port Entrance use case implemented in both Port of Valencia and Port of Livorno. Two different components are involved: Mobius OneM2M platform and a Pseudonymization

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

Module. The M2M platform is responsible for collecting meteorological data in Livorno seaport. DVL implements a RESTful connector/wrapper to interact with this platform, extracts the available data set, and exposes it by means of a RESTful API so that an AI-based platform can consume and correlate it with truck-turnaround times in the Livorno seaport. Moreover, within the same use case, a Pseudonymization Module component is used to process GateIn and GateOut events in order to identify personal data and pseudonymize it accordingly. The module retrieves the GateIn and GateOut events from the Port of Livorno by using existing RESTful APIs (available from Scenario 1), detects all the attributes which may be potentially sensitive (in our case the truck plate number), pseudonymizes the attribute according to available pseudonymization techniques (e.g., hash without key), and stores it within a conversion database. The DVL is able then to expose a RESTful API to allow an AI-based platform to consume pseudonymized data sets for training of predictive AI/ML models. The overall architecture for this scenario is depicted in the Figure 5:4 and further technical details can be found in deliverable **D6.2 PoC development, platform and test-bed integration** [18] and in deliverable **D5.3 Final iNGENIOUS data management framework** [19].

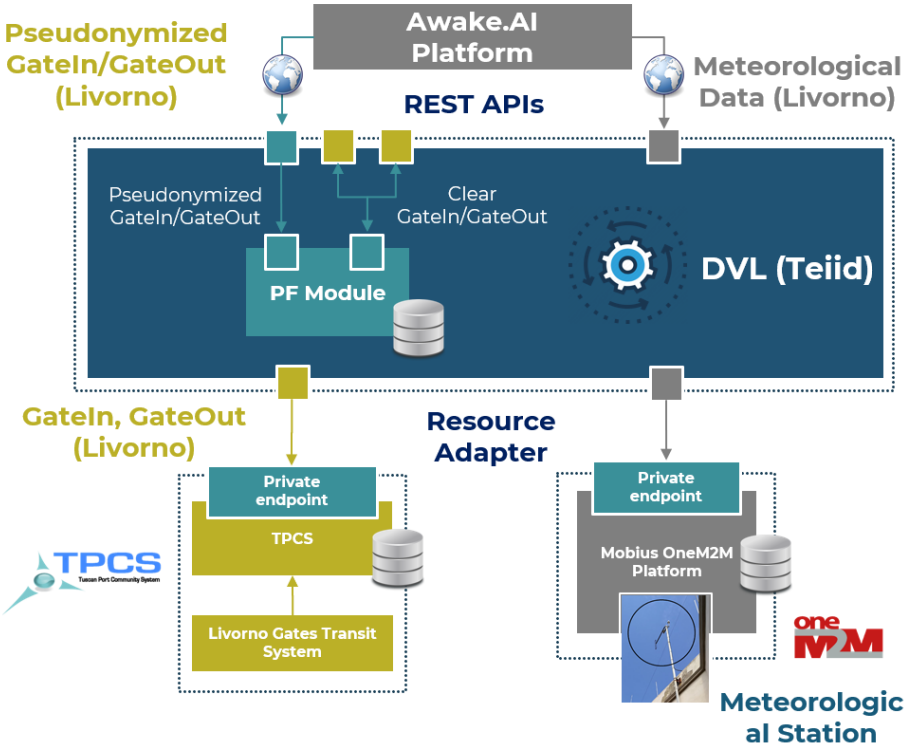

Figure 5:4: Data Virtualization Layer, Scenario 4 architecture

5.1.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

This subsection summarizes potential exploitable results for the Data Virtualization Layer in the context of DVL/DLT, Port Entrance and Ship use cases. Further information about the exploitation plans can be found in deliverable **D7.3 Final dissemination, standardization and exploitation** [3].

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

Component Group: M2M Platforms and DVL

Relevant for use cases: DVL/DLT, Port Entrance, Ship

Evaluation use case: DVL/DLT, Port Entrance, Ship

Test cases: UC4_TC_14, UC4_TC_15, UC5_TC_02, UC5_TC_05, UC5_TC_10, UC5_TC_11, UC5_TC_12, UC6_TC_01, UC6_TC_02, UC6_TC_03, UC6_TC_05, UC6_TC_06, UC6_TC_07, UC6_TC_08, UC6_TC_09, UC6_TC_10

Exploitation Potential:

- **CNIT:** iNGENIOUS allows validating the DVL component in relevant maritime scenarios by serving as a single access point for disparate data sources, which are part of the local data lake (e.g., M2M and third-party platforms, external data sources such as PCSs, etc.). By extending DVL capabilities with data pseudonymization functionalities, it will be possible to assess this approach for data access, retrieval, aggregation, and sharing against existing solutions. This will consolidate the adoption of a DVL component as a part of the overall ICT infrastructure in the port of Livorno for data access and management.
- **TEI**: Through iNGENIOUS, it will be possible to spread the technology results related to the data privacy and security aspects in distributed and heterogenous 5G/IoT/M2M based applications and services.
- **AdSPMTS**: iNGENIOUS outcomes are expected to be used to improve the available ICT stack and to strengthen the port digital capabilities of the Port of Livorno. The integration of real-time and off-line capabilities into the port community and monitoring platforms will enable services for a larger set of communities outside the project.
- **NXW**: iNGENIOUS has allowed to validate the use of Symphony in the Port of Livorno, thus practically assessing the capability of the platform to operate and support new type of deployments and environments, exploiting the interaction with DVL to transparently enable multiple and heterogeneous applications consume the collected data.
- **FV:** will leverage iNGENIOUS development and integration between M2M platforms and DVL to validate the potential of the exchange of data between PI System OSIsoft and external other data sources related to port management and operative events.

5.2 Component Group: DVL, Cross-DLT, and DLTs

One of the goals of iNGENIOUS is to provide a secure and trusted environment for data collection and distribution done by the Data Virtualization Layer (DVL). In particular, it is necessary to ensure that each port event such as GateIn, GateOut, Vessel-Arrival, Vessel-Departure, and Seal-Removal has a proof-of-integrity stored on blockchain and can be easily verified by end-users. To offer more decentralization and make the solution more interoperable, it is possible to register these events in different private and public Distributed Ledger Technology (DLT) networks. All this functionality is implemented within The Cross-DLT Layer.

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

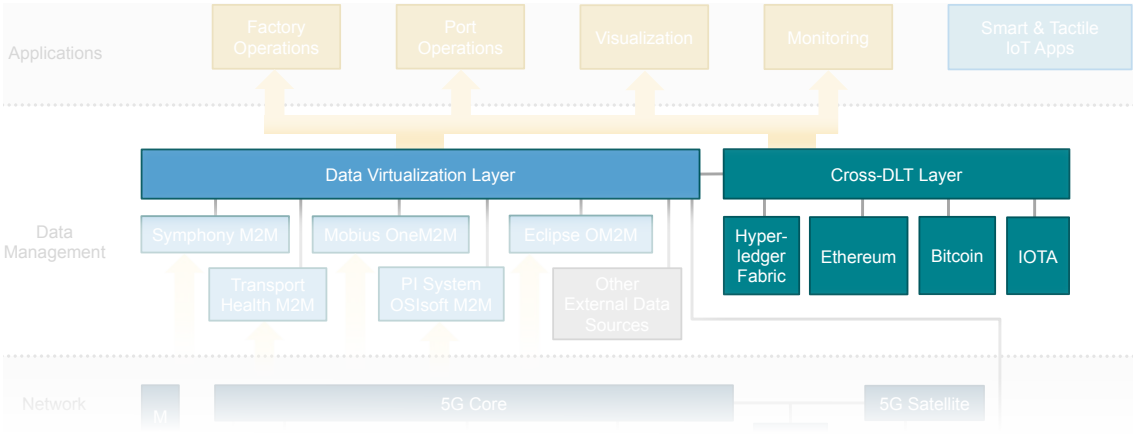

Figure 5:5: Component group consisting of Cross-DLT Layer and DLTs, integrating with Data Virtualization Layer

Cross-DLT Layer includes several interacting components. Firstly, a communication mechanism between DVL and Cross-DLT Layer is needed as the data that is stored on blockchain comes from different data sources and is processed by the DVL according to a certain data model. A communication bridge is provided to synchronize the data exchange between both layers. Therefore, the Cross-DLT Layer is now composed of two main components, TrustOS and the Integration Bridge. Telefonica's TrustOS is used as an orchestrator between DLTs networks in the sense of distributing data TrustPoints on user demand. Each DLT must implement a common REST API in order to store trust points in a standard way. Write and read methods are provided for the data producer (DVL) to store data and for consumers (any application) to request information for event display.

5.2.1 STATE OF THE ART BEFORE INGENIOUS

There are several types of DLT platforms or systems today. Each one has its own characteristics, but they all pursue the same objective, which is to provide a layer of trust through the immutable recording of data in a consensual and distributed manner. From the access rights perspective there are also different approaches. Privacy, performance, and security apply to permissioned networks, whereas security and transparency apply to public networks:

- Permissionless/public distributed ledger: Anyone can access and validate the information without the need for authorization from a central entity. Its nature is usually open source.
- Permissioned distributed ledger: The reading and validation of information must be authorized by certain entities or by the network.
- Hybrid distributed ledger: Leverage the advantages of public and permissioned ledgers by combining privacy, performance, security, and transparency.

There are several approaches to provide interoperability in the DLT world, for example, Polkadot, Hyperledger Cactus, Cosmos. Each has its benefits and tradeoffs. To use Polkadot one has to purchase its native token. Hyperledger Cactus is more like a framework for DLTs. Cosmos implements hub-and-spoke approach with its own token. But in fact, assets/events stored on one DLT cannot be deleted and/or moved to another DLT – by design ledgers are

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

immutable. Thus, iNGENIOUS provides its Cross-DLT solution by the ability to store hashes of the events on multiple DLTs.

5.2.2 INGENIOUS CONTRIBUTION AND INNOVATION

Innovation Summary: DVL, Cross-DLT, and DLTs
TrustOS: • Remove the underlying complexity of DLT • Interoperability between the different ledgers • Native integration with Ethereum and Polygon **DLT Common API:** • Ease of integration by any DLT based on the OpenAPI standard **Integration Bridge:** • Long polling mechanism between two passive REST-APIs which can manage information of different kinds **Benefit due to integration of the components:** • Increased trust, extended reach of the solution • Users may prefer some DLT technologies more than other • Combining multiple DLTs makes the solution attractive to a wider group of users • Storing proofs of events on several DLTs provides redundancy which increases the trust of users.

As mentioned in the previous section, the iNGENIOUS DLT layer seeks interoperability between different DLT platforms. To date, most projects involving distributed ledger technology choose a platform on which the immutable record of information will be trusted. The decision is closely linked to the requirements of the specific use case. For example, if a solution with a high number of transactions per second is needed, the most logical choice is a permissioned network. Thanks to the iNGENIOUS Cross-DLT Layer it is not necessary to choose a single platform, but the data can be stored in several DLTs and the end-user makes the decision.

To achieve this interoperability, it has been necessary to generate an architecture of components that interact with each other to achieve this goal. Each of them is detailed below to understand their main function and how they cooperate to bring innovation to the project.

TrustOS, DLT Common API and DLTs connectors: The main component in Cross-DLT Layer is Telefónica's TrustOS, a framework that removes the underlying complexity of blockchain technology in order to leverage its features in business processes. As explained in section 5.3 of deliverable **D2.2 System and architecture integration (Initial)** [1], TrustOS is a cloud-based software that provides the most demanded DLT features through functional modules. These modules are provided in the form of REST APIs to make their integration standard and as simple as possible. Specifically, the "Track" traceability module is used to store the information aggregated and offered by the DVL. Each piece of information that is recorded is modelled as a digital asset with a specific data model forming a trust point as integrity proofs.

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

TrustOS acts as a bridge to distribute the TrustPoints information between the different ledgers. To simplify the interaction, a common API has been implemented that each DLT has to implement to store the TrustPoints. This way, adding new DLT connectors is very easy and registration of TrustPoints is done in the same way in each DLT by making a single request to the DLT connector that complies with the common API.

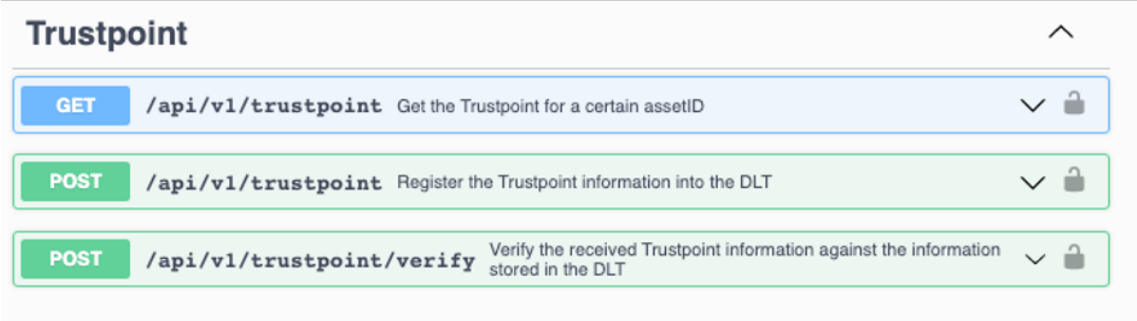

Figure 5.5: Common DLT API specific methods

Currently TrustOS has integration with the following technologies in the iNGENIOUS consortium context:

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

TrustOS offers native integration with Ethereum. Telefónica provides an Ethereum client node hosted by Infura.

As shown in Figure 5:6, TIOTBD also explored the capabilities of Polygon to include native integration. The main reason is the advantages of this platform compared to Ethereum, its performance, scalability and transaction costs. Polygon is a decentralised Ethereum scaling platform with increased scalability, performance and lower fees. It has full EVM compatibility which makes it possible to deploy smart contracts directly on the Polygon chain. Polygon uses a sidechain for fast transaction processing and stores checkpoints on the Ethereum mainnet to take advantage of both side features.

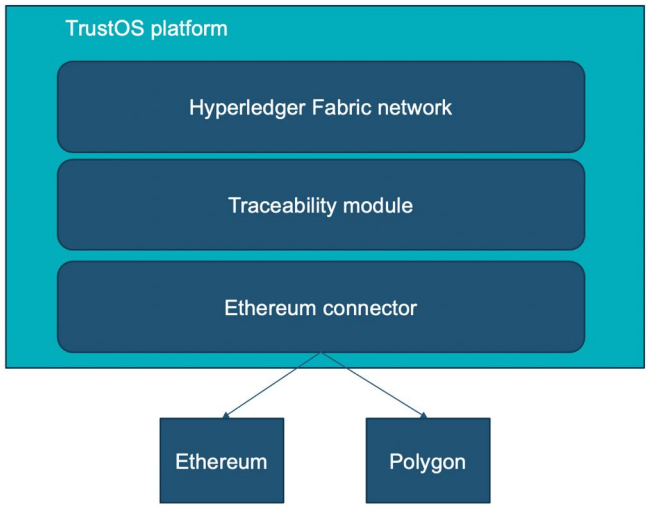

Figure 5:6: TrustOS native integration with Ethereum and Polygon

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

PJATK, FV, and CNIT have implemented the common interface in the form of DLT connectors for Bitcoin, Hyperledger Fabric, and IOTA, respectively, based on the OpenAPI standard because it defines a standard, language-independent interface for RESTful APIs.

Valencia port has also deployed a Hyperledger Fabric API with the objective of storing and exposing data related to GateIn and GateOut events at the Port of Valencia. The integration approach is visualized in Figure 5:7.

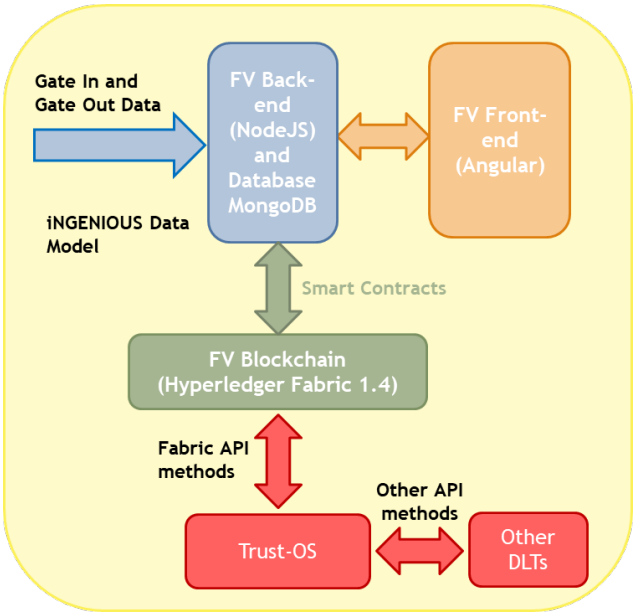

Figure 5:7: Port of Valencia Hyperledger Fabric interface to store GateIn and GateOut events

Integration Bridge: As introduced at the beginning of this section, the main problem with automating the registration of the information generated by the DVL to TrustOS is that both elements are passive elements, specifically REST APIs. Therefore, we need a mechanism that queries data in the DVL and stores it in TrustOS in an active way. This is the main reason for the implementation of the Integration Bridge.

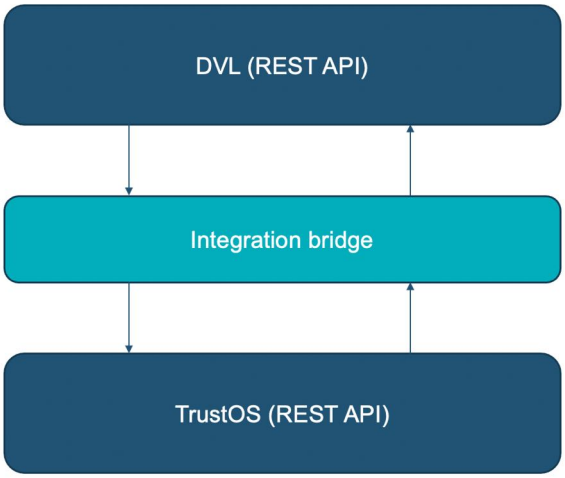

Figure 5:8: Integration Bridge between DVL and TrustOS

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

The three main goals of the bridge are:

- Act as an intermediate component between DVL and TrustOS.
- Use a long polling mechanism because it is one of the simplest ways of getting new information from the server with certain frequency.
- Model the event information coming from the DVL in the structure that TrustOS understands. TrustOS offers complete flexibility to represent any type of information, which is an advantage for the future if, for example, other types of events need to be stored.

The bridge asks the DVL frequently and actively if there are new events. The frequency is a parameter that can be customized depending on the requirements. If the information belongs to a new event, this event asset is created in TrustOS. If any information has already been registered for that event and it is new, an update is made on the asset.

5.2.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

Component Group: DVL, Cross-DLT, and DLTs
Relevant for use cases: DVL/DLT **Evaluation use case:** DVL/DLT **Test cases:** UC6_TC_04, UC6_TC_05 **Exploitation Potential:** • **TIOTBD:** The integration between TrustOS and different DLT connectors such as Bitcoin, IOTA/Tradelens and Hyperledger Fabric could be exploited to provide interoperability between DLTs in projects that need data immutability, trust, and security. • **PJATK:** Integration with DVL can be exploited as a joint solution to secure information from different sources such as IoT devices. • **FV**: The integration between TrustOS and Hyperledger Fabric, and the DVL and PI System OSIsoft will be exploited in future projects to enhance the interoperability of the IoT systems of the port of Valencia and other external systems.

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 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 have been developed, and their results provided for operational use through end-user applications like the one shown in Figure 6:1.

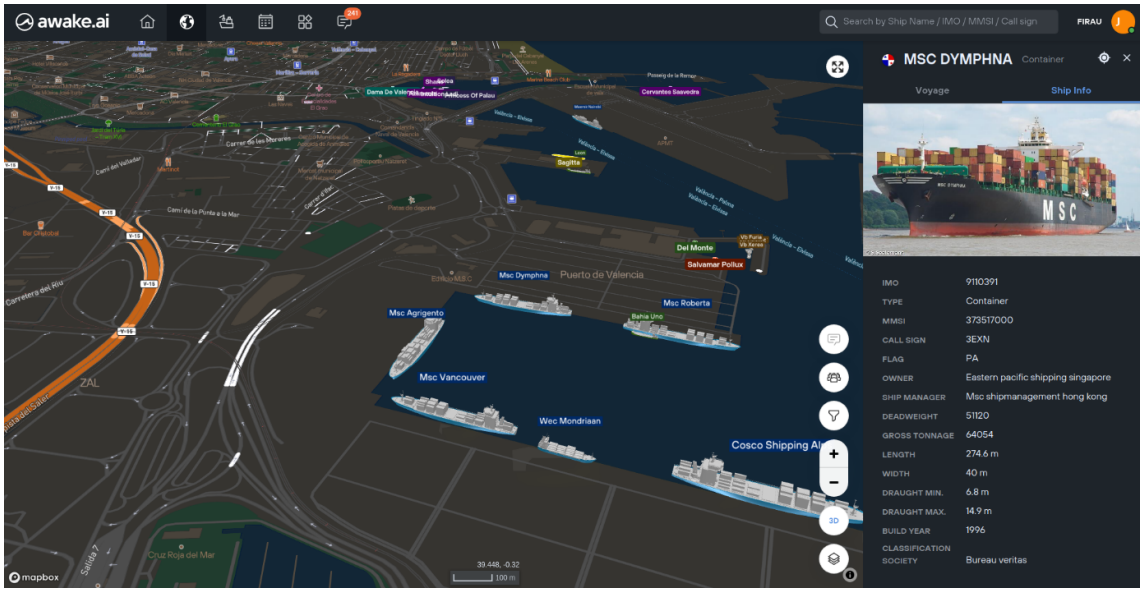

Figure 6:1: Awake.ai web application

The following Section 6.1 first describes how iNGENIOUS innovates on APIs for smart and tactile IoT applications in industrial environments. Section 6.2 then outlines the integration of system components to retrieve data from IoT sensor devices to APIs for providing information to the application layer in the iNGENIOUS architecture. This data is used in offline machine learning model development to build predictive models, and in online services and applications to provide actionable insight for increased operational efficiency.

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

6.1 Component Group: Application Programming Interface for Smart and Tactile IoT

The industrial tactile application programming interface (API) offers a set of functions that enable factory personnel responsible for developing automation routines to get data in and out of the system in a unified framework. Within this context, a number of available devices would exchange information through the API, which enables the user defined applications to exchange data easily and securely.

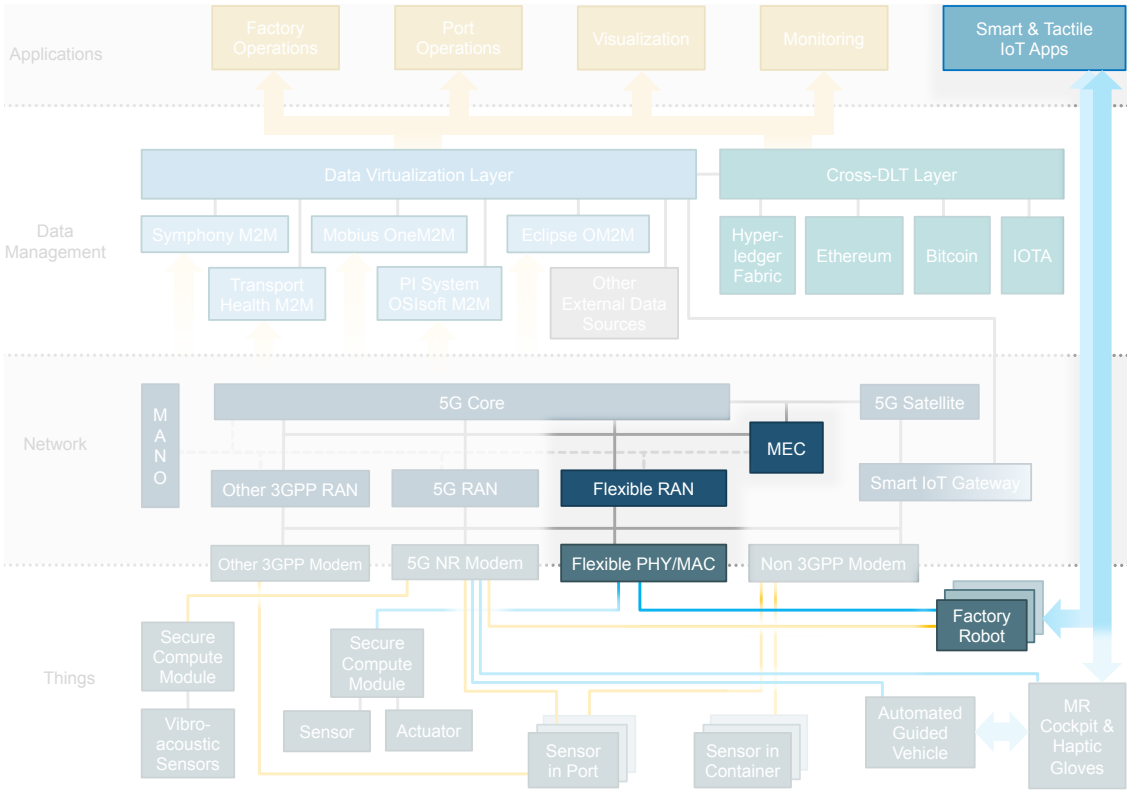

Figure 6:2: Cross-layer integration of smart IoT apps, remote controlling factory robots from an edge cloud

6.1.1 STATE OF THE ART BEFORE INGENIOUS

Smart and tactile IoT applications use input data that are the outcome of sensing and translate this information to actions performed by actuators. Replacing the employed wired communications in industrial sites by the wireless infrastructure is a challenging task when devices present multiple technologies that operate with different data structures and are expected to work in harmony. Efforts to mitigate this incompatibility have been made by the industrial and standardisation community, but no well stablished protocol is yet available.

Under this scenario, the available sensors and actuators within factory plants can be regarded as available manufacturing resources that can be programmed to produce specific products according to particular specifications. Further information on supply chain application types can be found in **Section**

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

3.2 of deliverable **D5.1 Key Technologies for IoT data management benchmark** [4].

6.1.2 INGENIOUS CONTRIBUTION AND INNOVATION

Innovation Summary: Application Programming Interface for Smart and Tactile IoT
Tactile IoT API: • Supports the flexibility and reconfiguration of the industrial production environment by providing seamless communication among components. **Benefit due to integration of the components:** • MANO assisted dynamic resource allocation in flexible PHY/MAC network through smart & tactile API • Data exchange between controller (5G modem) and cockpit on ASTI's AGV.

The industrial & tactile API proposed within the iNGENIOUS architecture provides different levels of abstraction:

1. An end user application development API, which gives the end user a simple and easily comprehensible graphical interface for instantiating new applications, and presents data in a format that is understandable by the end user
2. A mid-level function library, which contains functions that do not need to be directly used by the end user, such as an object detection algorithm
3. A low-level API that contains functions for data packets formatting and specification of communication link parameters given the requirements given by the end user.

These levels of abstraction are key aspects of the API, since they facilitate the employment of multi-access edge computing (MEC), which in turn allows the creation of industrial processes that require local computation for attaining latency constrains. The API was essential for allowing the integration between the flexible PHY/MAC network with the MANO as described in Section 4.1 of this deliverable, as well as the integration among the AGVs provided by ASTI and the cockpit from 5CMM.

6.1.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

An instance of one of the functions from the smart & tactile API is demonstrated within the Factory use case as it will be used for interfacing the resource allocation information provided by the MANO to the base station of the flexible PHY/MAC network. Detailed information on the integration between the orchestration entity and flexible PHY/MAC testbed network can be found in **Section 5.3** of **D4.4 Service orchestration at the edge** [16].

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

Component Group:
Application Programming Interface for Smart and Tactile IoT

Relevant for use cases: Factory

Evaluation use case: Factory

Test cases: UC1_TC_15, UC2_TC_04, UC2_TC_06, UC2_TC_07

Exploitation Potential:

- **TUD:** The integration among the upper layer components, such as MANO through the API with the flexible PHY/MAC will create a unique platform where the interaction and coexistence of non-3GPP radio access technologies can be investigated. This exploitation direction can contribute to the design of heterogeneous wireless networks that can be served by a common system at its network core. Moreover, the developed API will serve as easy connector for heterogeneous devices with the flexible PHY/MAC testbed.
- **ASTI:** The integration of advanced communication capabilities in AGVs and robots will enable real time information exposure and the development of smart orchestration industrial applications. ASTI will exploit these outcomes by offering new added value information services and including new control traffic capabilities in its solutions portfolio.
- **5CMM:** APIs and the unification of communication standards permit to connect multiple robots or AGVs to a common control platform or cockpit. 5CMM will exploit this work by improving the communication channel between cockpit and robot, enabling a more versatile and universal platform for different types of robots, all working under the same framework.

6.2 Component Group: DVL, Data Analytics, and Applications

For data analytics and applications, the main components are the DVL, data analytics, and application components in the use cases (traffic monitoring and data visualizations). The DVL provides data both for historical data analysis to train machine learning models, and online implementation of prediction services, data visualization, and monitoring operations in the supply chain.

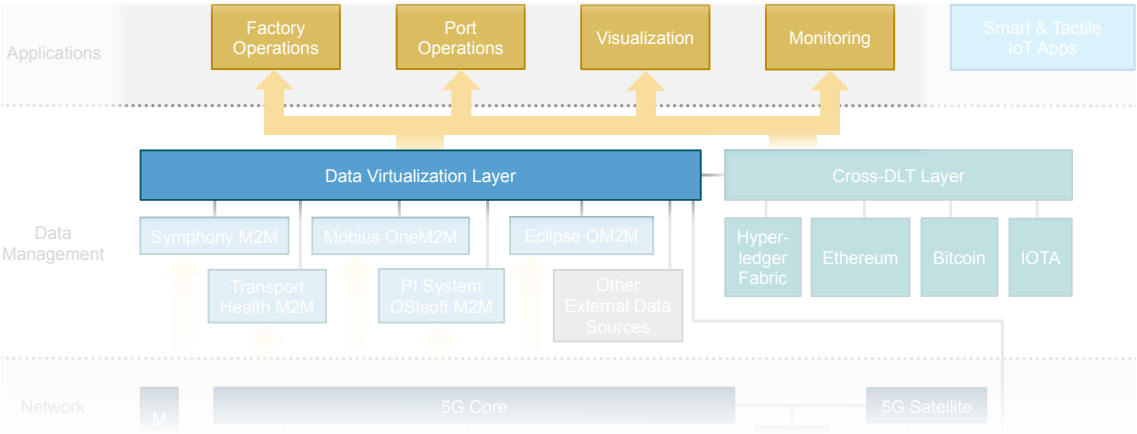

Figure 6:3: Applications built on top of the iNGENIOUS Data Virtualization Layer

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

6.2.1 STATE OF THE ART BEFORE INGENIOUS

Especially in the maritime supply chain, existing data analytics applications are largely focused on the operations of individual actors in the supply chain, such as vessel monitoring, route planning, terminal operations planning, or hinterland transport scheduling. IoT data is used in visualization applications to provide digital twin representations of static and dynamic resources for individual actors. In some areas such as vessel, truck, and train traffic monitoring, predictive models are also applied to estimate future events such as port arrival times. However, it is not common to share data between actors and digital systems, leading to a lack of shared holistic situational awareness over the supply chain, and inability to plan multimodal transport operations in an optimal way.

6.2.2 INGENIOUS CONTRIBUTION AND INNOVATION

Innovation Summary: DVL, Data Analytics, and Applications

Data Virtualization Layer (DVL):

- *See innovation summary table in Section 5.1.2*

Data Analytics:

- Building predictive models for port logistics processes and traffic patterns using heterogeneous data sources provided by the iNGENIOUS architecture

Applications:

- Communicating predictions and recommendations to logistic operators through end user applications to improve operational efficiency

Benefit due to integration of the components:

- The Data Virtualization Layer provides pseudonymization of potentially sensitive data elements, enabling more flexible data sharing across organisations for data analytics and holistic situational awareness.
- The data analytics components have access to holistic information across the multimodal supply chain, enabling modelling interdependencies between processes.
- Web applications provide visualization of current and predicted events and analytics across organization bounds.

In iNGENIOUS, FV, CNIT, and AWA collaborate to share and analyze holistic data on port operations in order to model the dependencies between multimodal traffic activities. This includes information on the movements of specific resources such as containers and trucks within the port, whose identification data is potentially sensitive. However, for traffic analysis it is generally not necessary to identify specific resources, but rather the correlations between traffic events and their timings. The DVL uses pseudonymization techniques to obfuscate the identities of resources, while allowing analysis of related events and interdependencies.

In data analytics for the port use case, interdependencies between vessel traffic and port calls, container operations in the port, and truck traffic events are analyzed and modeled. The goal is to produce predictive simulations of future

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

traffic rates and truck congestion based on up-to-date data sources such as public/commercial vessel tracking systems and pseudonymized port-specific data provided by systems such as the iNGENIOUS DVL. The system is designed to be modular in the sense that various characteristics of the port operations are modeled separately to allow predicting key variables (such as vessel port call schedules or cargo exchange volumes per port call) if relevant data is not available from external systems.

To provide a holistic view of the monitored and predicted traffic characteristics, online applications are developed to visualize the different data inputs and processes modeled using data analytics and received from the DVL. Figure 6:4 illustrates the kind of holistic situational awareness obtained from the system, showing global vessel traffic relevant for port of Valencia (top right), predicted container and truck traffic events (top left), aggregated truck/container traffic rates out of the port (bottom left), and truck turnaround time estimates for the port (bottom right). Additional applications and visualizations regarding smart and tactile IoT applications and truck tracking data visualization are presented in **Section 6.3** of **D2.2 System and architecture integration (Initial)** [1].

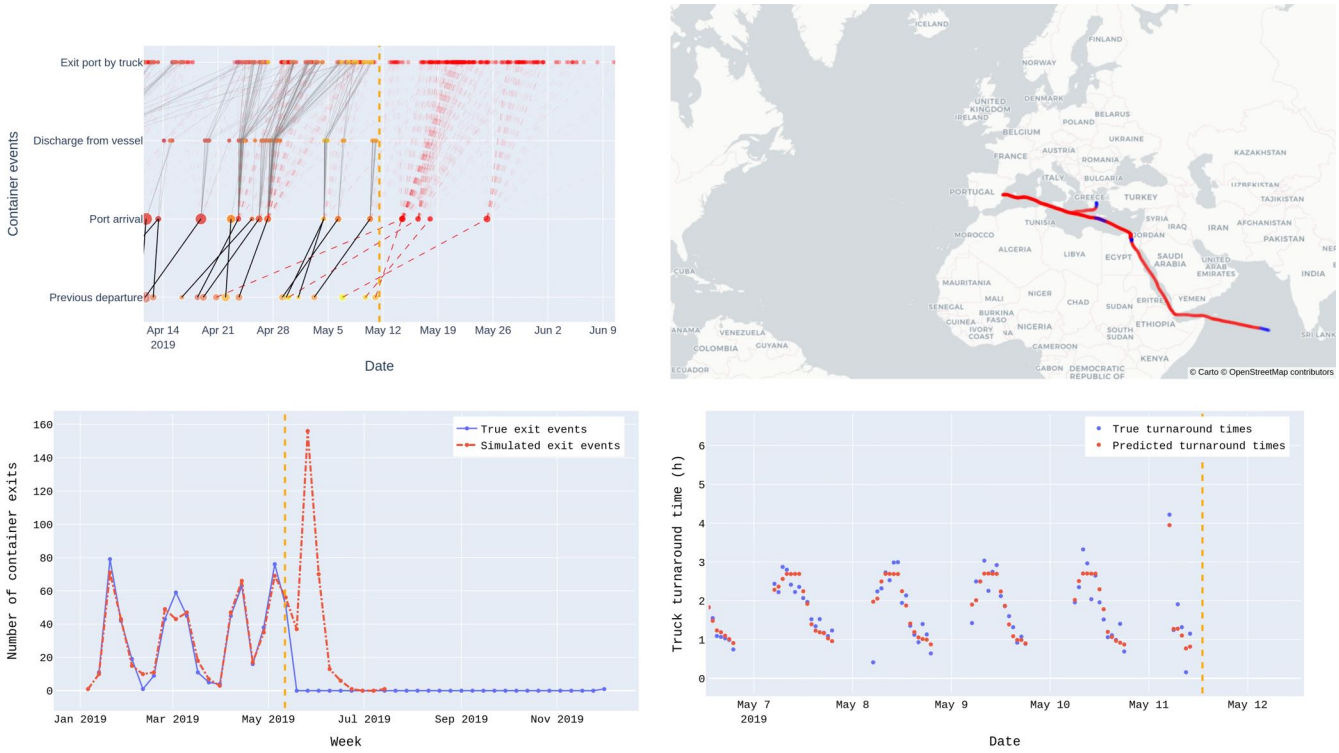

Figure 6:4: Visualization components for predictive analytics implemented in the port entrance use case

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

6.2.3 USE CASE COVERAGE AND EXPLOITATION POTENTIAL

Component Group: DVL, Data Analytics, and Applications

Relevant for use cases: Port Entrance

Evaluation use case: Port Entrance

Test cases: UC5_TC_01, UC5_TC_02, UC5_TC_03, UC5_TC_04, UC5_TC_05, UC5_TC_10, UC5_TC_11

Exploitation Potential:

- **AWA:** Commercialization of the model components developed as part of the port entrance use case. Global vessel schedule prediction models have already been developed into a commercial product during the project. Focus next on finding partners and customers for extending and applying the cargo operations prediction models to support commercial port operations planning. Awake.AI is actively pursuing opportunities to exploit the developed system as part of commercial pilots.
- **FV:** Leveraging use case results to analyse the added value obtained from aggregating multiple data sources to model operative conditions at the Port of Valencia. Exploiting results to show the potential of truck turnaround optimization in peak traffic times at the Port of Valencia. Sharing knowledge with other European and Non-European ports facing congestion problems. Sharing results related to the tracking of trucks inside the port facilities to show the potential of cellular IoT technologies in tracking use cases.
- **CNIT:** Technically evaluating the adoption of AI-based predictive models by assessing potential benefits and improvements for the supply chain in the context of the Port of Livorno. Extending the current set of IoT devices by deploying and integrating the new ones for monitoring purposes. Extending the partnership and collaboration with new industrial and commercial partners (e.g., services providers, equipment providers, mobile operators, etc.). Validating the usage of experimental components of the current ICT infrastructure adopted by the Port of Livorno (e.g., DVL, other M2M platforms, etc. Consolidating its role of technological enabler by assessing and supporting the transferability of the solution to other seaports.
- **AdSPMTS:** Assessing the possibility to integrate truck turnaround prediction models with the existing Digital Twin of the Port of Livorno as well as to further improve the capabilities of the Vehicle Booking System so that trucks' booking operations can be more efficient and optimized. Extending the current network of stakeholders (both private and public) by signing agreements with new commercial partners (service providers).

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

7 Use Case and Test Case Coverage

The iNGENIOUS architecture is generic and applicable to many different supply-chain and logistics use cases. In general, components at the things level are specific to certain use cases, whereas many components in the middle layers are shared and needed in all the use-case scenarios we consider. Unsurprisingly, some applications may target specific use cases, but all applications can employ DVL-supported data analytics techniques in similar ways.

Use Case Coverage and Integrations: The Data Virtualization Layer (DVL) developed in the DVL/DLT use case utilizes data models that have been defined in the Ship and Port Entrance use cases. Based on these data models, the DVL component can ingest real-time data produced by M2M components and other data sources that realize the Ship and Port Entrance use cases. However, due to complexity and the limited resources available to the project partners, not all components of the iNGENIOUS architecture can be fully integrated. Therefore, development, integration, and evaluation are done per use case. In Figure 7:1, we show which components and component groups the partners develop, improve upon, and evaluate within the six iNGENIOUS use cases. The components labelled "Other 3GPP Modem" and "Non-3GPP Modem" are not part of the evaluation, as consortium partners merely reuse them "off the shelf" as current state of the art (e.g., for the Smart IoT Gateway). However, in the case of Cellular IoT, partners contribute to the standardization with 3GPP.

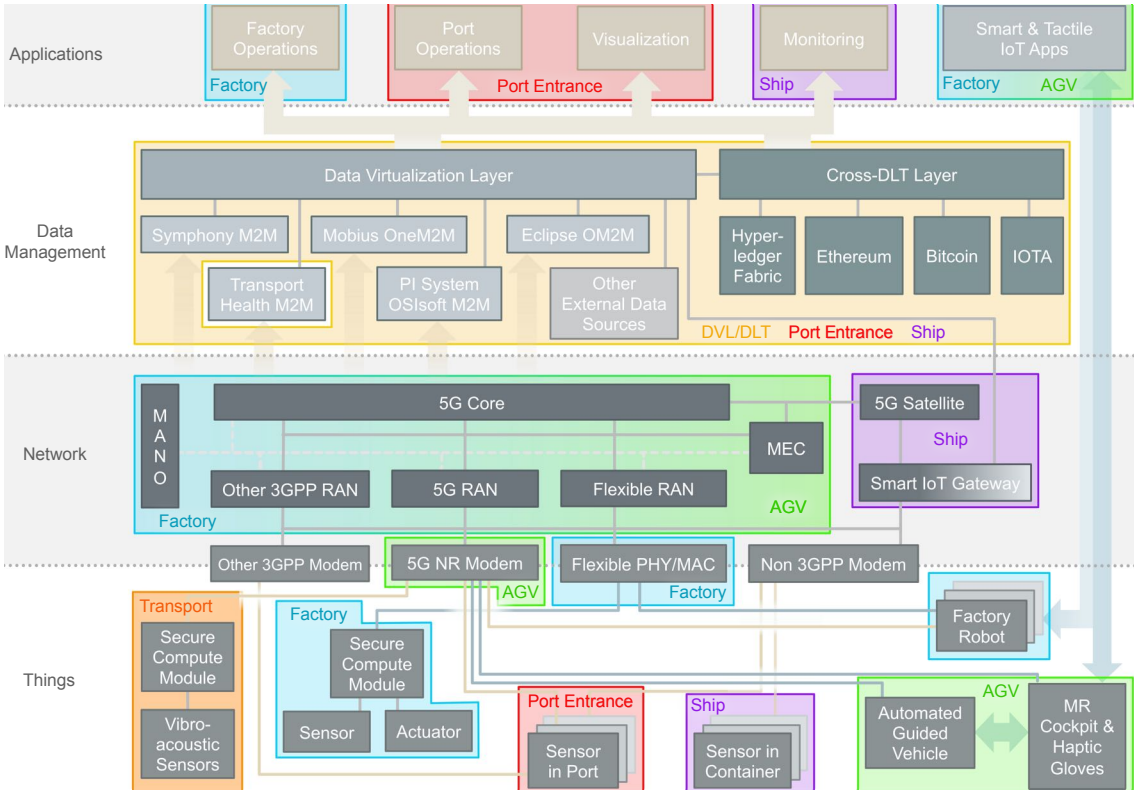

Figure 7:1: Use case and test coverage of components of the iNGENIOUS cross-layer architecture

In summary, the iNGENIOUS cross-layer architecture is implemented and evaluated at the use case level. The diagram in Figure 7:1 shows that almost all components are covered.

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

Test Coverage: The iNGENIOUS architecture will be evaluated based the test cases that have been identified in deliverable **D6.1 Initial planning for testbeds** [20]. The relevant test cases are listed in the "Use Case Coverage and Exploitation Potential" table for each component group described in this document. **Appendix A** of the D6.1 deliverable includes for each use case a simplified requirements traceability matrix that relates the test cases to the user and system requirements. The user and system requirements have been identified and described in deliverable **D2.1 Use cases, KPIs and requirements** [2]. To correctly map identifiers used in this document and **D6.1 Initial planning for testbeds** [20] to those used in D2.1, please see the mapping table in Section 1.2.

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

8 Conclusions

This deliverable, **D2.4 System and architecture integration (Final)**, describes the refined iNGENIOUS cross-layer architecture, following what has previously been reported in deliverable **D2.2 System and architecture integration (Initial)** [1].

This document provides an overview of the technical work conducted within the iNGENIOUS project. To this end, the role of and the main interactions between technological components of the overall architecture are summarized. Where appropriate, the text refers the reader to other technical deliverables that contain more detailed descriptions and discussions, namely deliverables D2.x, D3.x, D5.x, and D6.x.

The four main Chapters 3 through 6 of this document explain the key component groups within the architecture, highlighting the integration and cooperation of building blocks contained in each such group. For each component group, the partners provided summaries of the key innovations, including innovations that are enabled specifically as the result of integrating components, showing that they are "more than the sum of their parts". To put these innovations into perspective, they are described after a summary of the state of the art before the iNGENIOUS project. The exploitation potential is summarized, too, so as to help the reader assess business and research opportunities enabled by the project. The details of these aspects are left for another deliverable, namely **D7.3 Final dissemination, standardisation and exploitation** [3].

This version of the document summarizes the results of Task T2.2, which concludes in month M24 (September 2022) according to the work plan.

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

References

[1] “iNGENIOUS deliverable "D2.2 System architecture and integration (initial)",” 2021.

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

[3] “iNGENIOUS deliverabe "D7.3 Final dissemination, standardisation and exploitation",” 2022.

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

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

[6] “iNGENIOUS deliverable "D3.3 Secure, private and more efficient HW solutions for IoT devices",” 2022.

[7] D. Liu, “Baseband ASIP design for SDR,” *China Communications, vol. 12, no. 7,* pp. 60-72, July 2015.

[8] L. Drake, C. Zhaoyun and W. Wei, “Trends of communication processors,” *China Communications, vol. 13, no. 1,* pp. 1-16, January 2016.

[9] Z. Li, A. Nimr and G. Fettweis, “Implementation and Performance Measurement of Flexible Radix-2 GFDM Modem,” *2019 IEEE 2nd 5G World Forum (5GWF),* pp. 130-134, 2019.

[10] “iNGENIOUS deliverable "D3.4 Bio-haptic and XR-enabled IoT devices",” 2022.

[11] “iNGENIOUS deliverable D3.2 "Proposals for next generation of connected IoT modules",” 2022.

[12] “ORCA project,” [Online]. Available: https://www.orca-project.eu/.

[13] 3GPP, “TS-23502: Procedures for the 5G System (5GS)”.

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

[15] ETSI, “TS 128 530 R16”.

[16] “iNGENIOUS deliverable "D4.4 Service orchestration at the edge",” 2022.

[17] “iNGENIOUS deliverable "D5.2 Baseline iNGENIOUS data management framework",” 2022.

[18] “iNGENIOUS deliverable "D6.2 PoC development, platform and test-bed integration",” 2023.

[19] “iNGENIOUS deliverable "D5.3 Final iNGENIOUS data management platform",” 2023.

[20] “iNGENIOUS deliverable "D6.1 Initial planning for testbeds",” 2021.

[21] “iNGENIOUS deliverable "D4.5 Smart end-to-end iNGENIOUS IoT system",” 2022.

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