

fidal

field trials beyond 5G

D2.1: Requirements, Architecture and Methodologies

Lead beneficiary:	PNET	Contributors:	ADS, IQU, PSCE, ISI
Reviewers:	ADS, ISI		
Type:	Report	Dissemination:	Public
Document version:	V1.4	Due date:	M06, 30 06 2023

Project information

Project title:	Field Trials beyond 5G
Project acronym:	FIDAL
Grant Agreement No:	101096146
Type of action:	HORIZON JU Innovation Actions
Call:	HORIZON-JU-SNS-2022
Topic:	HORIZON-JU-SNS-2022-STREAM-D-01-01 SNS Large Scale Trials and Pilots (LST&Ps) with Verticals
Start date:	1 January 2023
Duration:	36 months

Document information

Associated WP:	WP2
Associated Task(s):	T2.1, T2.2, T2.3, T2.4
Main authors:	Charalabos Gizas, Christos Tranoris
Reviewers:	Charalambos Klitis (EBOS), Ishita Mishra (PIIU)
Type:	Report
Dissemination level:	Public
Due date:	30/06/23
Submission date:	30/06/23



List of Authors

Company	Author
ADS	Eric Munier
APART	Kostis Tzanettis, Michalis Sfakianos
EBOS	Charalabos Klitis
EKT	Didier Nicholson
FORTH	George Margetis
IQU	Kostas Ramantas
ISI	Elias Dritsas
NOVA	Ioannis Routis
ORAMA	Antonis Protopsaltis
OWO	Jorge Sianes Delgado
PSCE	David Lund, Katrina Petersen
STWS	Leonidas Perlepes, Alexios Pagkozidis
TID	David Artunedo Guillen, Jose Ignacio Hernadez Velasco
TNOR	Håkon Lønsethagen, Per Johny Nesse, Jane Pajo
UBI	Dimitris Manolopoulos, George Katsikas, Dimitris Klonidis
UMA	Almudena Diaz, Maria del Mar Moreno, José M. García-Nieto
UoP	Papaioannou Panagiotis, Apostolopoulos Takis

Disclaimer

The content of this document reflects only the author's view. The European Commission is not responsible for any use that may be made of the information it contains. While the information contained in the documents is believed to be accurate, the authors(s) or any other participant in the FIDAL consortium make no warranty of any kind with regard to this material including, but not limited to the implied warranties of merchantability and fitness for a particular purpose. Neither the FIDAL Consortium nor any of its members, their officers, employees or agents shall be responsible or liable in negligence or otherwise howsoever in respect of any inaccuracy or omission herein. Without derogating from the generality of the foregoing neither the FIDAL Consortium nor any of its members, their officers, employees or agents shall be liable for any direct or indirect or consequential loss or damage caused by or arising from any information advice or inaccuracy or omission herein.

Copyright message

© FIDAL Consortium. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both. Reproduction is authorised provided the source is acknowledged.

Table of Contents

List of acronyms and abbreviations	9
List of Figures:	15
List of Tables:	16
Executive summary	18
1. Introduction	19
1.1 Mapping FIDAL's outputs.....	19
1.2 Deliverable overview and document structure	21
2 Use Cases Introduction, Structure and Methodology	22
2.1 UC introduction.....	22
2.2 UC Definition Structure.....	23
2.2.1 Scenarios, contexts, and workflows	23
2.2.2 Stakeholders	23
2.2.3 How can beyond 5G networks benefit the Use Case	23
2.2.4 Technology needs	23
2.2.5 Key Performance Indicators (KPIs).....	23
2.2.6 Key Value Indicators (KVI)	23
2.3 UC methodology: KPI identification and associated process	23
2.3.1 State of the art.....	24
2.3.2 Identification of relevant key service KPIs.....	25
2.3.3 Mapping advanced Vertical Service KPI.....	28
2.4 UC methodology: KVI identification and associated process	31
2.4.1 State of the art.....	32
2.4.2 Key Values and Indicator Framework	38
2.4.3 KVI Methodology	45
2.5 UC methodology: Testing, experimentation, and validation of KPIs and KVIs	47
3 Use Case analysis overview	49
3.1 Market assessment, analysis, and feedback.....	49
3.1.1 Media vertical industries assessment.....	49
3.1.2 PPDR vertical market assessment.....	49
3.2 High-level use case description	49
3.2.1 Media vertical industries	49
3.2.2 PPDR vertical industries.....	51
4 UC1 – Internet of Senses/Haptic Sensing	54
4.1 Scenarios, contexts, and workflows	54
4.2 Stakeholders	55
4.2.1 Stakeholders' identification	55
4.2.2 Stakeholders' benefits	55
4.2.3 Stakeholders needs.....	55
4.3 How can beyond 5G networks benefit the UC	55
4.4 Technology needs	55
4.4.1 5G services needs	55
4.4.2 Network Application needs	56
4.4.3 Equipment needs.....	56



4.5	KPIs.....	56
4.6	KVIs.....	56
5	UC2 - Digital twin for first responders	58
5.1	Scenarios, contexts, and workflows	58
5.2	Stakeholders	58
5.2.1	Stakeholders' identification	58
5.2.2	Stakeholders' benefits	59
5.2.3	Stakeholders needs.....	59
5.3	How can beyond 5G networks benefit the UC	59
5.4	Technology needs	59
5.4.1	5G services needs	59
5.4.2	Network Applications needs	59
5.4.3	Equipment needs	59
5.5	KPIs.....	59
5.6	KVIs.....	60
6	UC3 – City security event / incident	61
6.1	Scenarios, contexts, and workflows	61
6.1.1	Scenario1: Critical infrastructure surveillance and inspection	61
6.2	Stakeholders	62
6.2.1	Stakeholders' identification	62
6.2.2	Stakeholders' benefits	62
6.2.3	Stakeholders needs.....	62
6.3	How can beyond 5G networks benefit the UC	63
6.4	Technology needs	63
6.4.1	5G services needs	63
6.4.2	Network Application needs	63
6.4.3	Equipment needs	63
6.5	KPIs.....	63
6.6	KVIs.....	64
7	UC4 – Advanced sports area media services	65
7.1	Scenarios, contexts, and workflows	65
7.1.1	Scenario 4.1: Enriched high quality video content collection and distribution	65
7.1.2	Scenario 4.2: Event media content extensions including end-user generated video material	65
7.2	Stakeholders	66
7.2.1	Stakeholders' identification	66
7.2.2	Stakeholders' benefits	66
7.2.3	Stakeholders needs.....	66
7.3	How can beyond 5G networks benefit the UC	67
7.4	Technology needs	67
7.4.1	5G services needs	67
7.4.2	Network Application needs	67
7.4.3	Equipment needs	67
7.5	KPIs.....	68

7.6	KVIs.....	68
8	UC5 – Virtual reality networked music performance	70
8.1	Scenarios, contexts, and workflows	70
8.1.1	Scenario 5.1: Remote playing of music.....	71
8.1.2	Scenario 5.2: Remote	71
8.2	Stakeholders	72
8.2.1	Stakeholders’ identification	72
8.2.2	Stakeholders benefits	72
8.2.3	Stakeholders needs.....	72
8.3	How can beyond 5G networks benefit the UC	72
8.4	Technology needs	73
8.4.1	5G services needs	73
8.4.2	Network Application needs	73
8.4.3	Equipment needs	73
8.5	KPIs.....	73
8.6	KVIs.....	73
9	UC6 – XR-assisted services for public safety.....	75
9.1	Scenarios, contexts and workflows	76
9.2	Stakeholders	77
9.2.1	Stakeholders’ identification	77
9.2.2	Stakeholders’ benefits	77
9.2.3	Stakeholders needs.....	77
9.3	How can beyond 5G networks benefit the UC	77
9.4	Technology needs	78
9.4.1	5G services needs	78
9.4.2	Network Application needs	78
9.4.3	Equipment needs	78
9.5	KPIs.....	78
9.6	KVIs.....	79
10	UC7 – Smart village engagement services.....	80
10.1	Scenarios, contexts, and workflows	80
10.1.1	UC scenario 7.1: Co-created engagement in urban communities.....	80
10.1.2	UC scenario 7.2: Co-created engagement in rural areas.....	80
10.2	Stakeholders	81
10.2.1	Stakeholders’ identification	81
10.2.2	Stakeholders’ benefits	81
10.2.3	Stakeholders needs.....	81
10.3	How can beyond 5G networks benefit the UC	81
10.4	Technology needs	81
10.4.1	5G services needs	82
10.4.2	Network Application needs	82
10.4.3	Equipment needs	82
10.5	KPIs.....	82

10.6	KVIs.....	82
11	Requirements elicitation via Focus Groups discussion.....	84
12	Agile User Stories.....	86
12.1	Infrastructure owners' User Stories.....	86
12.2	Use Case and Network Application owners' User Stories.....	87
12.3	Open Calls Stakeholders' User Stories.....	88
12.4	Experimenters User Stories.....	88
13	Overall architecture.....	90
13.1	Logical architecture of the FIDAL framework.....	90
13.2	Physical architecture of the FIDAL facility.....	94
13.2.1	Patras5G Testbed.....	94
13.2.2	Victoria Network Testbed.....	96
13.2.3	TNOR Testbed.....	97
14	Internal design of the FIDAL components.....	99
14.1	MAESTRO.....	99
14.1.1	Internal Architecture, Technologies, and baseline Assets.....	99
14.1.2	Functional Requirements.....	100
14.1.3	External APIs.....	100
14.1.4	Maestro Extensions throughout FIDAL.....	100
14.2	OpenSlice.....	101
14.2.1	Internal Architecture, Technologies, and baseline Assets.....	101
14.2.2	Functional Requirements.....	101
14.2.3	External APIs.....	102
14.2.4	OpenSlice extensions throughout FIDAL.....	102
14.3	AlaaS Component.....	102
14.3.1	Internal Architecture, Technologies, and Baseline Assets.....	103
14.3.2	Functional Requirements.....	103
14.3.3	External APIs.....	103
14.4	Monitoring Analytics.....	103
14.4.1	Internal Architecture, Technologies, and Baseline Assets.....	103
14.4.2	Functional Requirements.....	105
14.4.3	External APIs.....	105
14.5	FIDAL repository services.....	105
14.5.1	Internal Architecture, Technologies, and Baseline Assets.....	106
14.5.2	Functional Requirements.....	106
14.5.3	External APIs.....	106
15	Methodology for the vertical use case trial process.....	107
16	Security requirements, methodology, processes definition and guidelines.....	108
16.1	Requirements from the DoA.....	108
16.2	DoA FIDAL Security Declaration.....	109
16.3	DoA FIDAL Security Declaration.....	111
16.4	EU and National Regulatory and Standards Foundation.....	111
16.5	Driving Security Motivations.....	112

16.5.1	Trust and expertise viewpoint	112
16.5.2	Testbed viewpoint	113
16.5.3	Component domain viewpoint	114
16.5.4	Security from low TRL research, prototyping, field trials to live	114
16.5.5	Delivering for society	114
16.6	FIDAL Security Methodology	117
16.6.1	Security in different project contexts	117
16.6.2	Security Awareness across the project	118
16.6.3	Building trust across and beyond the project	119
16.6.4	Building resilience across and beyond the project	120
16.6.5	Maintaining a Library of Security Controls	121
16.6.6	Specific needs of the project	122
16.6.7	Needs of the verticals	123
16.6.8	Risk based approach to AI	124
16.7	Security Processes	125
16.7.1	Supply Chain considerations	125
16.7.2	Security Accreditation and Certification	125
16.7.3	Software Quality	126
16.7.4	Operational monitoring	126
16.7.5	Manual Risk Assessment	126
16.8	Summary and Conclusion of the FIDAL Security Methodology	128
17	Conclusion	129
18	References	130
Annex I:	131

List of acronyms and abbreviations

Abbreviation	Description
3D	Three Dimensional
3GPP	3 RD Generation Partnership Project
4G	4 TH Generation
5G	5 TH Generation
5GC	5 TH Generation Core networks
5GFoF	5G Factory of the Future
5G NR	5 TH Generation New Radio
5QI	5G Quality indicator
AI	Artificial Intelligence
AlaaS	Artificial Intelligence as a Service
AMF	Access and Mobility Management Function
AML	Adversarial Machine Learning
AoIP	Audio over Internet Protocol
API	Application Programming Interface
AR	Augmented Reality
B5G	Beyond 5 TH Generation
BSS	Business Support System
CAGR	Compound Annual Growth Rate
CAPIF	Common API Framework
CD	Continuous Deployment
CDF	Cumulative Distribution Function
CEA	Critical Entities Resilience
CI	Continuous Integration
CIRAS	Critical Infrastructure Risk Assessment Support
CMS	Configuration Management Server
cMTC	critical Machine Type Communications
CN	Core Network
COTS	Commercial out of the Shelf

CP	Control Plance
CPE	Customer Premises Equipment
CPS	Communication Service Provider
CSIRT	Cyber/Computer Security Incident Response Team
CU	Centralized Unit
CVD	Coordinated Vulnerability Disclosure
DAG	Directed Acyclic Graphs
DL	Downlink
DNS	Domain Name System
DRL	Deep Reinforcement Learning
DU	Distributed Unit
E2E	End to End
EDGEAPP	Edge Applications
emBB	Embedded Broadband
EMF	Electro Magnetic Field
eNB	Evolved Node B
ENISA	European Agency for Cyber Security
EPC	Evolved Packet Core
ETSI	European Telecommunications Standards Institute
EU	European Union
FoF	Factory of the Future
Gbit/s	Gigabits per second
GDPR	General Data Protection Regulation
GMS	Group Management Server
gNB	Next-Generation Node B
GPU	Graphics Processing Unit
GSMA	Global System for Mobile Communication Association
HD	High Definition
HMD	Head Mount Display
HUD	Head Up Displays

HVS	Human Visual Systems
HW	Hardware
Hz	Hertz
IaaS	Infrastructure as a Service
IBV	Institute for Business Value
ICT	Information and Communication Technology
IdMS	Identity Management Server
IMT-2020	International Mobile Telecommunications 2020
IoT	Internet of Things
IP	Internet Protocol
IPR	Intellectual Property Rights
ITU	International Telecommunications Union
JPEG	Joint Photographic Experts Group
K8s	Kubernetes
KMS	Key Management Server
KPI	Key Performance Indicator
KPIEE	Key Value Indication Energy Efficiency
KVI	Key Value Indicator
KVM WG	Kernel-based Virtual Machine Working Group
LCM	Lifecycle Management
LEA	Law Enforcement Agents
LMLC	Low Mobility Large Cell
LNaaS	Logical Network as a Service
LTE	Long Term Evolution
MAE	Mean Absolute Error
MANY	Mobile Access North Yorkshire
Mbit/s	Megabits per second
MCDData	Mission Critical Data
MCMCC	Mission Critical Multimedia Communication and Collaboration
MCPTT	Mission Critical Push TO Talk

MCS	Mission Critical Services
MDA	Mobile Data Access
MEC	Multi-Access Edge Computing
ML/DL	Machine Learning / Deep Learning
MOCN	Multi Operator Core Network
MOS	Mean Opinion Score
MR	Mixed Reality
MSE	Mean Square Error
MSKPI	Media Service Key Performance Indicator
MSP	Managed Service Providers
MVP	Minimum Viable Product
NCOM	NOKIA Cloud Operations Manager
NEF	Network Exposure Function
NFV	Network Function Virtualization
NFVOs	Network Functions Virtualization Orchestrator
NIS2	Network and Information Security
NMP	Network Music Performance
NOrc	NOKIA Orchestrator Center
NSaaS	Network Slice as a Service
NSDs	Network Service Descriptors
NSI	Network Slice Instance
NTN	Non-Terrestrial Networks
NTP	Network Time Protocol
OECD	Organisation for Economic Co-operation and Development
O-RAN	Open Radio Access Network
OSM	Open-Source Management and orchestration
OSS	Operation Support System
PaaS	Platform as a Service
PCM	Pulse Code Modulation
PEVQ	Perceptual Video Quality of Experience

PLMN	Public Land Mobile Network
PPDR	Public Protection & Disaster Relief
PQI	Perceptual Quality Index
PSKPI	Public Protection & Disaster Relief Service Key Performance Indicator
QA	Quality Assurance
QoE	Quality of Experience
QoS	Quality of Service
R&D	Research and Development
R&I	Research and Innovation
RAN	Radio Access Network
RBAC	Role Based Security Control
RIT	Radio Interface Technology
RTT	Round Trip Time
SA	Situation Awareness
SA	Standalone
SBI	Service Broker Interface
SDK	Software Development Kit
SDR	Software Defined Radio
SDU	Service Data Units
SIP	Session Initiation Protocol
SLA	Service Level Agreement
SME	Small Medium Enterprise
SMF	Session Management Function
SMPTE	Society of Motion Picture and Television Engineers
SNO	Single Node OpenShift
SNR	Signal to Noise Ratio
SRIT	Set of Radio Interface Technologies
SW	Software
T&M	Testing and Monitoring
TaaS	Testing as a Service



TBD	To Be Determined
TMV WG	Test, Measurement and Validation Working Group
TOM	Themes Outcomes and Measures
TRL	Technology Readiness Level
TRxP	Transmission Reception Point
UAS	Unmanned Aerial Systems
UC	Use Case
UE	User Equipment
UGC	User Generated Content
UHD	Ultra-High Definition
UK	United Kingdom
UL	Uplink
UPF	User Plane Function
uRLLC	Ultra Reliable Low Latency Communications
V2X	Vehicle to Infrastructure Communications
VM	Virtual Machine
VPN	Virtual Private Network
VQM	Video Quality Model
VR	Virtual Reality
WP	Work Package
XR	Extended Reality
Zt-DE	Zero touch Decision Engine

List of Figures:

Figure 1: Hexa-X Digital World.....	24
Figure 2: 6G goals and improvements over 5G.	27
Figure 3: Technology areas with strong impact on different 6G requirements and KPIs.	28
Figure 4: FIDAL Repository structure.	46
Figure 5: Agile development methodology and validating of KPIs and KVI.	47
Figure 6: UC1 Workflow Diagram 1.	54
Figure 7: UC1 Workflow Diagram 2.	55
Figure 8: UC2 Workflow Diagram.	58
Figure 9: UC3 Workflow Diagram.	62
Figure 10: Example of a Networked Music Performance	70
Figure 11: Data interaction overview for UC5.	71
Figure 12: UC6 Workflow Diagram 1.	75
Figure 13: UC6 Workflow Diagram 2.	76
Figure 14: Stakeholder (citizen or city/rural community official) operating on digital twins and real time coordinating of incidents in rural areas using VR capabilities.	80
Figure 16: : FIDAL Logical Architecture Diagram.	90
Figure 17: FIDAL's Deployment plan.	91
Figure 18: PNET/NOVA pre-commercial network extension.....	95
Figure 19: Patras5G Architecture diagram.	95
Figure 20: Victoria Network (Malaga's testbed).....	96
Figure 21: Telenor LST architecture.....	98
Figure 22: Maestro's high-level architecture.....	99
Figure 23: OpenSlice Architecture.	101
Figure 24: Data Analysis Pipeline.....	103
Figure 25: Monitoring Analytics platform internal architecture.	104
Figure 26: FIDAL Repository Services internal design.....	106
Figure 27: Onboarding lab testing and trials methodology.....	107
Figure 28: Who trusts who? What trusts what?.....	113
Figure 29: Holistic security view.	114
Figure 30: Abstract component domains.	114
Figure 31 Components of the FIDAL security methodology.....	118
Figure 32: EC Risk based approach to AI Regulation.	124
Figure 33: Risk Management approach.	127
Figure 34: Factors of risk assessment.	127
Figure 35: Interdependent risk assessment on the technical and information layers.....	128
Figure 36: Energy efficiency in NFV on data transfer [9].....	137

List of Tables:

Table 1: Adherence to FIDAL Deliverable & Task Descriptions	19
Table 2: FIDAL Use Cases and key participants.....	22
Table 3: 5G vs. B5G/6G network architecture.....	28
Table 4: Guidelines understanding your contribution.....	38
Table 5: KVIs and Trustworthy.....	38
Table 6: KVIs and Inclusiveness.....	39
Table 7: KVIs Fairness.....	39
Table 8: KVIs and Personal Freedom.....	39
Table 9: KVIs and Transparency.....	39
Table 10: KVIs and Privacy.....	40
Table 11: KVIs and Economic Sustainability.....	40
Table 12: KVIs and Business Value.....	40
Table 13: KVIs and Tackling economic inequality.....	41
Table 14: KVIs and Responsibility.....	41
Table 15: KVIs and Open collaboration.....	41
Table 16: KVIs and Flexibility.....	41
Table 17: KVIs and Environmental Sustainability.....	42
Table 18: KVIs and Waste Management.....	42
Table 19: KVIs and Mitigation Strategies.....	43
Table 20: KVIs and Compliance Quality Standards.....	43
Table 21: KVIs and Safety.....	43
Table 22: KVIs and Security.....	43
Table 23: KVIs and Data Protection.....	44
Table 24: KVIs and Societal sustainability.....	44
Table 25: KVIs and Healthier community.....	44
Table 26: KVIs and Cultural connection.....	44
Table 27: KVIs and Knowledge.....	45
Table 28: KVIs and Quality of Living.....	45
Table 29: Target technological KPIs for UC1.....	56
Table 30: KV's of initial potential relevance for UC1.....	56
Table 31: Target technological KPIs for UC2.....	59
Table 32: KV's of initial potential relevance for UC2.....	60
Table 33: Target technological KPIs for UC3.....	63
Table 34: KV's of initial potential relevance for UC3.....	64
Table 35: Target technological KPIs for UC4.....	68
Table 36: KV's of initial potential relevance for UC4.....	68
Table 37: Target technological KPIs for UC5.....	73
Table 38: KV's of initial potential relevance for UC5.....	74
Table 39: Target technological KPIs for UC6.....	78
Table 40: KV's of initial potential relevance for UC6.....	79
Table 41: Target technological KPIs for UC7.....	82
Table 42: KV's of initial potential relevance for UC7.....	83
Table 43: Table of User Requirements.....	84
Table 44: Infrastructure owner Persona.....	86
Table 45: Infrastructure owner user stories.....	87
Table 46: Network Application developer persona.....	87
Table 47: Network application developer user stories.....	87
Table 48: Open call Participant Persona.....	88
Table 49: Open Call Participant User Story2.....	88
Table 50: Experimenter's persona.....	89

Table 51: Experimenter's user story.	89
Table 52: List of FIDAL Network Applications.	93
Table 53: FIDAL architecture interfaces and APIs.	93
Table 54: Basic radio site configurations.	98
Table 55: Supported TM Forum APIs.	98
Table 56: Maestro's functional requirements.	100
Table 57: OpenSlice's functional requirements.	101
Table 58: Functional Requirements of AlaaS Component.	103
Table 59: Functional Requirement of Monitoring Analytics.	105
Table 60: FIDAL Repository functional requirements.	106
Table 61: initial suggested KVis for security.	115
Table 62: 5th percentile user spectral efficiency.	135
Table 63: Average spectral efficiency.	136



Executive summary

FIDAL promises to deliver a platform and necessary enablers that will support advanced and ambitious 5G advanced use cases targeting the augmentation of human capabilities, allowing Media & PPDR vertical industry players to perform advanced technological and business validation in large-scale field trials of highly innovative and advanced applications that exploit Evolved 5G technologies, while it needs to adapt to the emerging 5G challenges and the open calls that are planned by FIDAL. This document lays the foundation for establishing the groundwork necessary for realizing the concepts of FIDAL. By conducting detailed analyses, addressing security considerations, integrating beyond 5G towards 6G technologies and services, defining open interfaces, adapting the architecture, and establishing repositories, it provides the essential guidelines and infrastructure for the successful execution of large-scale use cases on the FIDAL fabric. The use cases in focus are aimed at assessing the potential of beyond 5G technology in the Media and PPDR vertical industries, with a consideration of societal aspects and key value indicators (KVI).

The FIDAL use cases in the context of the Media vertical industries are as follows:

- UC1: Internet of senses/haptic sensing
- UC4: Advanced sports area media services
- UC5: Virtual reality networked music performance
- UC7: Small village engagement services

The FIDAL use cases in the context of the PPDR vertical industries are as follows:

- UC2: Digital twin for first responders
- UC3: City security event/Incident
- UC6: XR-assisted services for public safety

1. Introduction

This document lays the foundation for establishing the groundwork for the implementation of the innovative concepts that form the foundation of the FIDAL initiative. Its primary objective is to conduct a comprehensive analysis and detailed definition of the requirements and designs necessary to enable the execution of large-scale use cases on the FIDAL fabric. By leveraging and building upon previous and ongoing work from EU-funded 5G-PPP and SNS projects, this document aims to establish a solid framework for the successful deployment of FIDAL's 5G labs and facilities.

One of the key objectives of this work is to align the specific requirements of the use cases with the overarching FIDAL architectural approach. This entails a careful examination of how the key value indicators (KVI) and key performance indicators (KPI) can be effectively employed to drive the realisation of FIDAL's objectives. By incorporating these performance metrics, the described work ensures that the large-scale trials conducted on the FIDAL fabric are in line with the project's strategic goals and deliver measurable results.

Considering the criticality of security in large-scale trials, this document places special emphasis on studying and addressing any potential security implications. Through thorough analysis and the formulation of guidelines, FIDAL developments aim to provide a secure environment for the execution of the trials. By considering various methods and processes, the work seeks to mitigate risks and establish robust security measures that protect the integrity and confidentiality of the FIDAL infrastructure.

Another significant objective of FIDAL is to define seamless integration processes for novel experimentation tools and advanced 5G technologies. By enabling the provision, orchestration, and management of the large-scale trials, the FIDAL platform facilitates the effective utilisation of these cutting-edge tools and technologies. Additionally, this document explores the integration of novel FIDAL services such as AI as a Service and Security as a Service within the experimentation process and operation during the trials. This integration ensures that the trials benefit from the latest advancements in AI and security technologies, enhancing their effectiveness and overall outcomes.

To encourage collaboration and innovation, this document defines a set of open and extensible interfaces. These interfaces will allow for the seamless integration of third-party solutions from the open calls process. By promoting openness and interoperability, FIDAL encourages a diverse ecosystem of solutions and stimulates the emergence of novel ideas and approaches within the FIDAL project.

As the requirements from the large-scale trials and the open calls partners evolve, there is a need to undertake the task of refactoring and adapting the FIDAL architecture in an iterative manner. This adaptive approach ensures that the project remains agile and responsive to the evolving needs and challenges encountered during the trials. By continuously improving the architecture, our work enables the efficient utilisation of resources and maximises the potential of the FIDAL infrastructure.

Finally, the document describes the setting up of FIDAL repositories. These repositories serve as centralised repositories of lessons learnt, resources, and documentation related to the FIDAL project. They facilitate easy access to information and promote collaboration among project stakeholders, ensuring efficient information exchange and promoting a shared understanding of the project's goals and progress.

1.1 Mapping FIDAL's outputs

The purpose of this section is to map FIDAL Grand Agreement commitments, both within the formal deliverable and Task description, against the project's respective outputs and work performed.

Table 1: Adherence to FIDAL Deliverable & Task Descriptions

Project GA Component Title	Project GA Component Outline	Respective Document Chapter (s)	Justification
TASKS			

<p>Task 2.1 – Definition and detailed analysis of vertical use cases and applications, baseline and corresponding target KVs and KPIs, and service requirements</p>	<p>This task aims to provide a detailed definition of the vertical use cases in the Media and PPDR domain, including their scenarios descriptions, infrastructure requirements, and alignment with project objectives. It involves specifying demonstrated beyond 5G functionalities, target KPIs and KVs, and expected service requirements.</p>	<p>Section 2-10</p>	<p>Sections 2 and 3 include the definition structure for the use case description in terms of stakeholders, service needs and target KPI and KVs. Sections 4-10 includes the analysis of each use case.</p>
<p>Task 2.2 – Requirements, analysis, and specifications of the end-to-end FIDAL architecture</p>	<p>This task will identify and requirements and map them to functional requirements of the system to derive the technical specifications of the FIDAL components and overall experimentation framework.</p>	<p>Sections 11-14</p>	<p>Sections 11 and 12 include the requirement elicitation methodology and the identified requirements mapped to functional requirements of the system. In sections 13 and section 14 we present the overall logical and physical architecture of the platform and the testbeds that will host and support the execution of the large-scale trials and open calls.</p>
<p>Task 2.3 – Security requirements, methodology, processes definition and guidelines</p>	<p>The purpose of this task is to define the requirements, methodology, processes, and guidelines for the security work package in the FIDAL project. It involves centralising knowledge of risk assessment processes, conducting a project-wide risk assessment, integrating security into the design process, and providing ongoing guidance and oversight.</p>	<p>Section 16</p>	<p>Sections 16 describes the processes, methodology and guideline for the FIDAL security framework.</p>
<p>Task 2.4 – FIDAL repositories development & methodology for the vertical use cases trial process</p>	<p>This task focuses on defining methodologies and databases for comprehensive trials of beyond 5G technologies and vertical use cases. It includes specifying test cases, measuring performance, and developing a repository for lessons learned and technical assets.</p>	<p>Section 2.5 Section 14.5 Section 15</p>	<p>Sections 2.5 and 15 present the methodology for vertical use case trials. Section 14.5 provides a detailed description of the FIDAL repository services.</p>

1.2 Deliverable overview and document structure

The document is organised into sections that address different aspects of the project. Here's an overview of the sections included:

- **Sections 2 to 10** of the deliverable document focus on defining and analysing the vertical use cases and applications. They describe the scenarios, prerequisites, and infrastructure requirements, and establish target KPIs and KVIs. These sections also explain how the use cases align with the project objectives and showcase the demonstrated functionalities.
- **Sections 11 to 12** of the document specifically address the requirements, analysis, and specifications of the end-to-end FIDAL architecture. In these sections, we conduct use case stakeholders' requirement elicitation, ensuring that their needs and expectations are captured. Additionally, we map non-functional requirements to functional requirements and system specifications, ensuring that the architecture meets the necessary criteria for optimal performance and usability.
- **Sections 13 to 15** focus on presenting the logical and physical architecture of FIDAL, along with the description of the FIDAL components. Additionally, these sections outline the FIDAL repositories and the methodology for conducting vertical use case trials. They provide insights into the structure and organisation of FIDAL, as well as the approach taken for testing and evaluating its effectiveness in specific use case scenarios.
- **Section 16** of the deliverable document is dedicated on defining the security requirements, methodology, processes, and guidelines. This part of the documentation emphasizes the importance of incorporating security measures throughout the design process. This section also outlines the specific security considerations and requirements that need to be addressed, ensuring the confidentiality, integrity, and availability of the system. It also highlights how security is integrated into the overall design, emphasizing the implementation of best practices and industry standards to safeguard the project against potential threats and vulnerabilities.

Together, these sections form a comprehensive document structure that captures the essential elements of the project, from use case analysis to architecture design and security integration.

2 Use Cases Introduction, Structure and Methodology

2.1 UC introduction

The purpose of the advanced FIDAL Use Cases (UCs) is to assess the capabilities of beyond 5G technology for the Media and PPDR vertical industries to enable their commercial exploitation considering all respective societal aspects and KVIs as well. During the project's conception phase, FIDAL performed a stakeholders' preliminary risk-analysis for the UCs and generated the descriptions for the identified use cases. As such, verifying the key target beyond 5G KPIs and KVIs in the content of those industry segments is expected to motivate a very high standardisation, societal, business, and economic impact. Each UC will deploy a layered testing practice to drive development, involving significant industry representative tests, verifications, and validations: (i) tests using specific use cases oriented for dedicated single or multi-concurrent vertical industries, and (ii) test, measurements, validation, and demonstration in the large-scale infrastructures.

However, being the first technical deliverable of the FIDAL project, the document also presents a distilled view of the project's scope and objectives and highlights the innovations and ambitions that are set to be fulfilled. It delves into the technological solutions that are part of FIDAL aiming at clarifying how the project will build on the existing technologies. In this context, the deliverable is expected to serve as a fundamental reference guide for specifying the FIDAL system architecture and determining the subsequent implementation work.

The core objectives of this work include:

- a) Thorough description of the scenarios and context in which they take place.
- b) List of pre-requisites and assumptions (technical or nontechnical).
- c) Description of each scenario-specific Infrastructures.
- d) Positioning with respect to FIDAL's objectives.
- e) Demonstrated functionalities for the UCs.
- f) Target KPIs and KVIs and expected service requirements for each UC.

The FIDAL use cases and their key participants are listed in Table 2.

Table 2: FIDAL Use Cases and key participants.

	UC title	Vertical	Key Participants	Testbed/Large scale Infrastructure
UC1	Internet of senses/haptic sensing	Media	OWO , UMA, TID	UMA, TID
UC2	Digital twin for first responders	PPDR	SAT , UoP, PNET, NOVA	UoP, PNET, NOVA
UC3	City security event/Incident	PPDR	ADS , UMA, TID	UMA, TID
UC4	Advanced sports area media services	Media	NOVA , UoP, PNET	UoP, PNET, NOVA
UC5	Virtual reality networked music performance	Media	TNOR , EKTA, IQU	TNOR
UC6	XR-assisted services for public safety	PPDR	ORAMA , FORTH, UoP, PNET, NOVA	UoP, PNET, NOVA
UC7	Small village engagement services	Media	TNOR	TNOR

2.2 UC Definition Structure

The structure of each use case scenario description has been defined to ensure coherency and ease-of-readability for the reader. A summary of each sub-section within the use case scenario description is provided below.

2.2.1 Scenarios, contexts, and workflows

In this section, we explore each use case in depth to uncover the specific challenges, requirements, and goals involved in their implementation. We also highlight the practical applications and potential benefits that these use cases can bring to the FIDAL project, and the people involved in it. Each UC presents a workflow and outlines actions and sequential steps to accomplish the intended functionalities or result.

2.2.2 Stakeholders

Each UC identifies the stakeholders listed below:

- Stakeholders from the media and PPDR sector;
- Citizens;
- Developers of Network Applications;
- Telecom Operators;
- Testbed and infrastructure owners.

2.2.3 How can beyond 5G networks benefit the Use Case

Each Use Case will elucidate the rationale behind the utilisation of FIDAL solutions, highlighting the necessity to surpass the usage of 5G or previous radio access technologies. This analysis will encompass the challenges and limitations associated with such an approach.

2.2.4 Technology needs

Based on the stakeholders' analysis, each UC provides the technology needs required to fulfil the targeted scenarios. The following needs have been identified as relevant:

- 5G services' needs;
- Network Applications' needs;
- Advanced Vertical Services' needs;
- Equipment's' needs.

2.2.5 Key Performance Indicators (KPIs)

Each UC provides indicative target technological KPI values to be validated in each of their trials.

2.2.6 Key Value Indicators (KVI)

Each UC provides indicative target KVI values.

2.3 UC methodology: KPI identification and associated process

The scope is to identify (based on architectural elements analysis, information flow, etc.) the potential impact on the service performance and user perceived quality. The challenge is to understand the relative influence of 5G evolution network performance indicators to the vertical services. The KPIs mapping methodology includes four steps:

1. Research on definitions and information derived from 5G-PPP, standardisation bodies and respective alliances e.g., ITU and NGMN, as well as definition of use cases from H2020 projects.
2. Identification of relevant key service KPIs and their definitions that are of importance to the respective industry.
3. Mapping of advanced vertical service KPIs to the appropriate 5G evolution network KPIs that impact the service provision process.

4. Perform lab, large-scale trials for both FIDAL and open calls UCs measuring both service and network KPIs to prove the correlation, the targets, and areas for improvement. Such result will be a valuable input to both standardisation bodies and vendors.

These target KPI values have been obtained from standardization bodies (e.g., ETSI 3GPP, NMG, ITU) as well as from the consortium vendors' & members' expertise and experiences.

2.3.1 State of the art

I. European Vision for the 6G Network Ecosystem¹

According to the study, the key features of 6G will include intelligent connected management and control functions, programmability, integrated sensing and communication, reduction of energy footprint, trustworthy infrastructure, scalability, and affordability.

The 6G architecture should be sufficiently flexible and efficient to enable easy integration of everything, i.e., a network of networks, joint communication and sensing, non-terrestrial networks, and terrestrial communication, encompassing novel AI-powered enablers as well as local and distributed compute capabilities. The use of AI everywhere in the network, where it can be beneficial, i.e., the "AI everywhere" principle, will be used to enhance network performance and to provide AI-as-a-Service in a federated network. AI and Machine Learning will help to maintain operation cost-effectiveness of envisioned complex 6G services, such as the interaction on human-digital-physical worlds and Internet of Senses, to automate some level of decision-making processes, and to achieve a zero-touch approach.

II. Hexa-X^{2 3}

The Hexa-X project that was funded under the EU H2020 framework is a flagship project that develops the B5G/6G vision and intelligent fabric for connecting human, physical and digital worlds. One of the main objectives of Hexa-X is to define the 6G KVI and a framework that will allow the quantitative assessment of the impact that 6G will have on society.

The Hexa-X vision for 6G revolves around interactions between three worlds: a human world of our senses, bodies, intelligence, and values; a digital world of information, communication, and computing; and a physical world of objects and organisms. The future 6G network system should make it possible for these worlds to tightly synchronise and integrate to make it possible to seamlessly move between them. Realising these interactions will open many new use cases, applications, and services that will benefit people on all levels: as consumers, parts of enterprises or societies.



Figure 1: Hexa-X Digital World.

¹ <https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf>

² Hexa-X project deliverable D1.2: https://hexa-x.eu/wp-content/uploads/2021/05/Hexa-X_D1.2.pdf

³ Hexa-X Use cases and Key value indicators. Url: https://www.youtube.com/watch?v=N_bUAGkzz-8

III. TMV Working Group

The Test, Measurement, and KPIs Validation (TMV) Working Group was founded as part of the 5G PPP effort to promote commonalities across projects that have strong interest in Testing & Monitoring (T&M) methodologies needed to provide support to the vertical use cases in 5G Trial Networks. Such efforts include the development of test and measurement methods, test cases, procedures as well as the KPI formalisation and validation to the greatest possible extent, to ensure a unique European vision on how the entire lifecycle of the 5G network, ranging from R&D to actual deployed environments, can be supported.

The white paper [TMV-Results-Explanation-White-Paper-V1.0]⁴ targets at clarifying the details behind the performance numbers and at providing a series of interpretation guidelines that could help the reader better understanding the 5G domain. In the white paper there will be identified what are the main impact factors that affect the results and provide a high-level explanation that is clearly understandable by non-experts.

The KPIs considered to compare 4G & 5G are bandwidth, peak data rate for uplink, peak data rate for downlink, user experience data rate for uplink, user experienced data rate for downlink, user plane latency, control plane latency, reliability, and area traffic capacity.

2.3.2 Identification of relevant key service KPIs

KPI Clustering Methodology

The TMV WG define a KPI methodology in the white paper Beyond 5G/6G KPIs and Target Values⁵

To provide a harmonised and formalised view of the B5G/ 6G KPIs across projects a three-step methodology was followed by the TMV WG. As first step, the TMV defined the information to be collected by the research projects, related to the KPIs definitions, target values, as well as information relevant to the context of these definitions. In particular, the information to be collected have been the following:

- **KPI Category**, referring to the targeted KPIs category for example: Data Rates and Capacity, Latency, Mobility, Reliability and Availability, or other categories.
- **KPI Name**, given in the context of the project.
- **KPIs Definition**, detailed to ensure understanding of the true nature of the KPI.
- **Use case/ context of the KPIs**, including details related to the context of a specific Proof of Concept. Enhancement related to the KPI target value.
- **Information on where/how the KPIs will be measured**, referring to the layer/ the reference points where measurements will be collected.
- **Any known information on the influence quantities of the KPI**, being “the quantities that are not the measurand but that affects the result of the measurement” [1].
- **Relative or absolute evaluation of the KPIs**
- **Other relevant information (e.g., Standardisation references)**

To capture the ICT-52 projects’ view on the KPIs, and not influence the results by means of predefining the KPI definitions and targets based on external references, the projects were asked to directly provide input (that is available at this stage) on the above.

⁴ <https://5g-ppp.eu/wp-content/uploads/2021/08/TMV-Results-Explanation-White-Paper-V1.0.pdf>

⁵ https://5g-ppp.eu/wp-content/uploads/2022/06/white_paper_b5g-6g-kpis-camera-ready.pdf

With the collection of the responses and the aggregation and streamlining of the information the TMV WG further clustered the KPIs in several KPI families representing the ICT-52 projects vision on key B5G/6G qualities. These families are the following:

- **Latency:** “Latency” is usually defined as the contribution of a network unit to the time from when the source sends a packet to when the destination receives it. A network unit can be a network segment or processing node (implemented as SW or as HW). Based on this definition, the “Latency KPIs” category defined in the context of this work includes all KPIs that refer to latency or to latency components (contribution) of various segments/ functions/ components, at various planes; namely user plane, control plane and orchestration plane in the performance of various application of network functionalities/processes. This classification has taken under consideration besides the standardised KPI definitions the work performed in [1], and [3] on the decomposition and definition of the latency contributions in 5G networks.
- **Capacity:** The “Capacity” KPIs category refers to metrics that are used to evaluate the amount of network resources provided to end-users. From this perspective, the “Capacity KPIs” category includes KPIs evaluating the bandwidth resources provided per user (i.e., user data rate), the bandwidth resources provided per area surface or node (i.e., node capacity, area traffic density, etc.), and the number of connections/devices that can be served per area (i.e., connection density); as being multiple metrics of the network resources capability.
- **Packet Loss:** The “Packet Loss” KPIs category refers to KPIs used for evaluating the packet transmission success rate of a system to transmit defined amount of traffic within a predetermined time. Packet Loss and Frame Loss are also considered as success rate measure of a transmission system.
- **Compute:** Computing resources are expected to play a major role in the performance of B5G/6G networks, beside communication and storage resources. The “Compute” KPIs category reflects the importance of computing elements, and the fact that the use of computing resources is determinant in 6G implementation, usage, and performance.
- **Energy:** Energy KPIs family refers to KPIs used for evaluating the energy efficiency of a system. This system can be the B5G/6G network, the user device or even a VNF responsible for specific functionalities. The ultimate target in all KPIs is to decrease the energy consumption of the system.
- **Security:** This KPI family covers KPIs related to security, anomaly detection and privacy. The KPIs are defined at different levels and are meant to be evaluated at different segments, and between different endpoints in B5G/6G systems.
- **Channel:** The “Channel” KPIs family refers to KPIs specifically addressing the evaluation of the communication channel and the efficiency of the use of the physical channel resources.
- **Electric and Magnetic Fields (EMF):** This KPI family covers KPIs related to Electric and Magnetic Fields (EMF) - and refer to measures of exposure to it.
- **Localisation:** This KPI family addresses aspects of B5G/6G networks regarding the localisation accuracy.
- **Service Availability and Reliability:** This KPI family cover KPIs related to service availability and reliability. The service not being specifically defined it can cover different entities, related to different domains.

Following this clustering, the standardised KPI definitions from international and European Standardisation Organisations such as ITU-R, 3GPP and ETSI - and target values set available in previous generation networks - were reviewed and used as reference for the relevant KPI families. Main families addressed are Capacity related (Peak Data Rate, User Experienced Data Rate, Area Traffic Capacity, Connectivity Density), Latency related (User Plane and Control Plane latency), Reliability, Energy Efficiency related (including Energy Efficiency in NFV) and positioning related. These definitions are repeated in the following chapter.

A detailed description of KPI is available in annex I, section A.

Beyond5G/6G KPI

According to the white paper⁶, over the last decade we have seen a 50% to 100% yearly growth in mobile data traffic volume. There is no reason to assume that the next decade this growth of mobile data will slow down. We can expect a continued increase of the number of connected devices (sensors, connected cars, home devices, body cams, etc) combined with ever increasing demands from new applications and services. This implies that 6G will have to cater for a mobile data traffic volume that is up between 100x to a 1000x larger than 5G. Note that this growth of mobile data traffic volume cannot result in a comparable growth in energy consumption. To keep energy consumption of 6G comparable to 5G, overall energy use per terminal, base station, network node must come down and energy efficiency per transported and processed data needs to improve in line with the growth of mobile data traffic volume.

One of the biggest promises of the next decade is that immersive communication, holographic telepresence, and AR/VR will become our default way of communication. It is commonly agreed that the ideal quality for such immersive experience will require 8k video resolution per eye. To support this kind of applications we expect that 6G will have to deliver end user experienced data rates up to 10 Gbits/s.

The increasing number of mobile devices does not necessarily mean that the mobile device density increases. However, 6G will likely use smaller cells in which the device density can be higher. 6G should support peak densities of up to 10 devices per m². Furthermore, when the mobile data traffic for each device increases, the required capacity will also increase. For scenarios such as spectators in a stadium with augmented reality glasses or workstations on an office floor, capacities in the range of 150 Tpbs/km² will be needed, which means 10x the capacity requirements of 5G. Figure 2 shows an overview of the main 6G goals, plus the KPIs where 6G will be improving 5G.

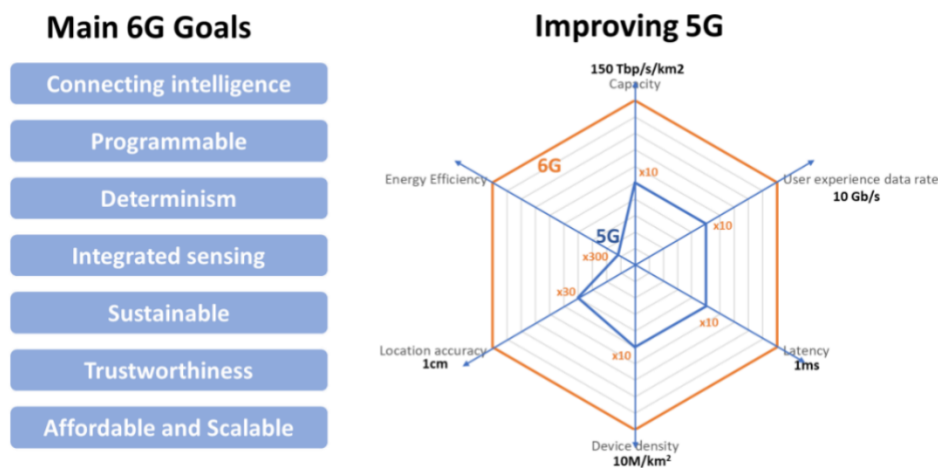


Figure 2: 6G goals and improvements over 5G.

This study highlighted the envisaged key technologies for 6G, ranging from system network architecture and control, edge and ubiquitous computing, radio technologies and signal processing, optical networks, networks and service security, non-terrestrial networks communication, as well as devices and components (Figure 3 shows these technology areas with strong impact on different 6G requirements and KPIs).

⁶ <https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf>

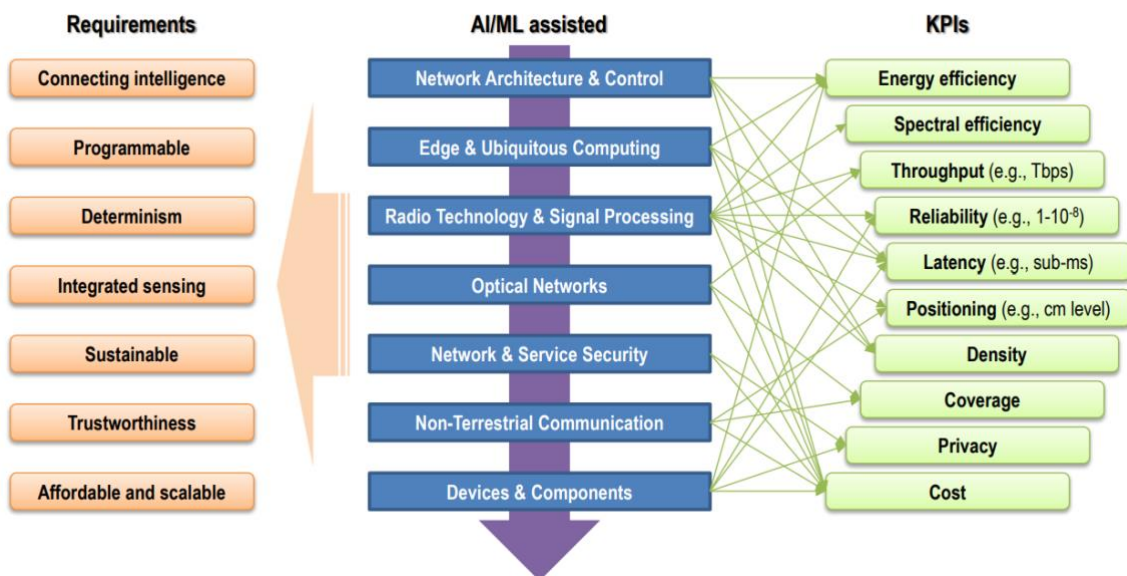


Figure 3: Technology areas with strong impact on different 6G requirements and KPIs.

The envisioned main differences between 5G and B5G/6G network architecture can be summarised in the following table:

Table 3: 5G vs. B5G/6G network architecture.

TYPE OF SERVICE	Point to point QoS transport	Point-to-multipoint transport, including configurable logical network overlay topologies with managed quality properties and network application awareness, with compute services, sync services, AI services
TYPE OF RESOURCES	Communication	Communication + compute + sensing
ARCHITECTURE SCOPE	RAN +CN	Terminal + RAN + CN
CLOUD-NATIVE	Only CP in 5GC	E2E and cross plane (User plane / Control plane / Management plane)
MICROSERVICES	No	Yes, E2E, all planes
RESOURCE AWARENESS	Only in air interface	Yes, all employed resources, including compute, transport, wireless
TRUSTWORTHINESS	Trustworthy nodes	Trustworthy adaptive service/ network of networks
AM/ML INTEGRATION	Over-the-top	Natively integrated
ADMISSION CONTROL	Access control	Execution control
DEVICE/NODE DISAGGREGATION	CU/DU, IAB	Fully flexible

2.3.3 Mapping advanced Vertical Service KPI

FIDAL will integrate in the facility sites several innovative advanced 5G technologies enablers, the following sub-chapters listed some of the services that may be deployed in the facilities sites depending on the use cases requirements.

I. Secure AI as a Service

Security will be implicit within FIDAL AlaaS provision as it has been indicated by a previous work for enabling privacy-preservation and security⁷. FIDAL will leverage this strength, providing advanced infrastructure, lowering cost, and reducing the need for development teams to have machine learning expertise. AlaaS provides an opportunity to combine top-down, drawing from vertical sector requirements, with bottom-up approaches that take advantage of innovative technical capabilities. FIDAL also seeks to innovate in terms of human engagement, seeking views and experiences of Network Applications developers. Future ecosystems will be collaborative and inclusive⁸. This is an end to end overarching view, highlighting the importance of demonstrating application reliability. Thus, a holistic security approach will provide safe and secure services, building trustful cooperation FIDAL and Network Application developers⁹. Security considerations for AlaaS include data security, reliability, transparency, data governance, and accessibility (i.e., speech, text, vision, analytics, translation and searching) of end points¹⁰. These should be considered as algorithms and ML models are designed. FIDAL also draws from existing ethical guidance regarding the use of automated decision-making in services¹¹, seeking to identify harm caused by unintended outcomes, service discrimination, a lack of responsible oversight, unsafe data handling and compliance failures.

II. AI as a Service

FIDAL, in addition to facilitating validation of highly innovative use cases, also serves as a playground of rapid prototyping and validation for forward-looking applications grounded with QoE and PPDR. This is made available with a set of vertical-specific Network Applications, and a set of AI libraries, SDKs, and tools. A key contribution in this direction is the construction of an API Serving comprising a set of ML/DL methods which support the distributed data processing and analysis as well as the secure federation of scalable AlaaS (i.e., Fed ML/DLServing) by using the distributed PyTorch¹² and the distributed TensorFlow¹³ combined with the multiple workers of Keras¹⁴. AutoML methods will be developed^{15 16} for predictive modelling on the specific nature of each vertical. These methods will cover the collection and curation of datasets (to be leveraged by vertical application developers) oriented to the Network Applications deployment and operation, the selection of important significant variables, and the adoption of self-tuning and self-adaptive data analytic pipelines. In addition to these, justification mechanisms with confidence score leading to explainable AI will be deployed for informed decision making of AI-outputs. The AI Tool which will combine all the libraries is fourfold: i) seamless integration, confluence and execution of AI models training and serving; ii) support of scriptable/coding notebooks putting more power in the end user's hands (i.e., data scientists/engineers, applications developers) compared to the existing opaque solutions¹⁷; iii) abstraction of coding details to define a collection of reusable containerized AI models in the form of binary images (i.e., by means of Network Applications) to author human-centric data analytic pipelines by means of Directed Acyclic Graphs (DAGs); and iv) reproducible AlaaS applications and better integration with underlying stacks and infrastructures. These methods will be validated in the context of large-scale pilots considered in FIDAL and considering the general and specific KPIs and KVI of the orchestration environment. Network Applications are chains of application enablement VNFs that implement vertical-specific functions on top of the NFVI, abstracting its details, and are part of the Network Slice Instance (NSI) chain. Thus, they act as a middleware layer with reusable functions for a certain vertical domain (e.g., video streaming for Media) which helps reduce service creation time. Using metrics for Evaluating the machine

⁷ Ericsson Research (2021), Hexa-X Use cases and Key value indicators. Url: https://www.youtube.com/watch?v=N_bUAGkzz-8

⁸ Reuters Plus (2022), Beyond 5G, Japan's collaborative approach to next-gen networks. Url: <https://www.reuters.com/brandfeature/beyond-5g-japans-collaborative-approach-to-next-gen-networks>

⁹ NTT(2022)https://www.docomo.ne.jp/english/binary/pdf/corporate/technology/whitepaper_6g/DOCOMO_6G_White_PaperEN_v4.0.pdf

¹⁰ contenteratechspace – TechBlogger (2020), Artificial Intelligence as a Service – AaaS. Url: https://www.youtube.com/watch?v=_Jzn8JTdue8

¹¹ UK Cabinet Office (2021), Ethics, Transparency and Accountability Framework for Automated Decision-Making. Url: <https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making/ethicstransparency-and-accountability-framework-for-automated-decision-making>

¹² https://pytorch.org/tutorials/beginner/dist_overview.htm

¹³ https://www.tensorflow.org/guide/distributed_training

¹⁴ <https://www.tensorflow.org/tutorials/distribute/keras>

¹⁵ Thornton et al (2013), Auto-WEKA: combined selection and hyperparameter optimization of classification algorithms. Url: <https://dl.acm.org/doi/10.1145/2487575.2487629>

¹⁶ <https://automl.github.io/auto-sklearn/master/>

¹⁷ colab.research.google.com

learning algorithms is an essential part of the project. Specifically, for assessing the robustness of the AI algorithms minimum MSE or MAE will be used for regression models while for classification models the maximum classification accuracy and logarithmic loss metrics are going to be used for discovering the balance in the number of training epochs, omitting over-fitting.

III. Zero touch service

The technologies used, namely Maestro, OpenSlice¹⁸ and PaaS toolkit are mature technologies developed in the last years in several European projects and supported many Verticals using the 5G Systems as well as Network Applications platforms. These platforms in FIDAL will be integrated to provide an advanced system that will both provision FIDAL UC applications as well as prepare and operate the FIDAL fabric for large scale trials, but also it will enable all future technologies arriving from the Open calls process. Artificial intelligence (AI)-driven Zero-Touch management will be adopted as a new paradigm to enable self-organised infrastructures on large scale trials, where scalable AI architectures can be designed to monitor, analyse, and take data-driven decisions at both local and global scopes autonomously, while allowing for a practical large-scale deployment. This approach will be applied in large field trials for the first time, adapting the Zero-Touch concept being developed at the ICT-20 MonB5G and ICT-52 MARSAL projects. Core to the design of the Zero Touch concept is a series of distributed Reinforcement Learning (RL) agents, deployed at Service Orchestrator and the Operation Support System (OSS) to control the operation of Service Management and Slice management respectively. Each RL agent solves an optimisation problem via Deep Reinforcement Learning, which minimises the convergence time towards meeting the corresponding objective (e.g., latency minimisation at the RAN domain, appropriate computation capacity allocation to applications). To address inter-dependencies between different technological domains FIDAL will support the coordination of RL agents via a novel centralised Zero Touch Decision Engine (Zt-DE). The Zt-DE will monitor RL agents, making arbitration decisions to solve race conditions or conflictive decision making due to cross domain trade-offs. It can also enact changes on DRL objective functions, to adapt to different operating conditions and performance objectives. The FIDAL Service Orchestrator and OSS/BSS, are based on two mature assets, the Kubernetes-based Maestro and the OpenSlice OSS/BSS, that will be integrated and upgraded with Zero Touch functionality for the first time within FIDAL.

IV. Catalogue of reusable assets and Network Apps Service

A Service Catalogue Repository will be leveraged from the 5GMediaHUB project and extended to support a comprehensive index of searchable and reusable assets. These include (a) the list of Network Applications along with their constituent VNFs, metadata and interfaces, including Northbound APIs and standardized SBIs (Southbound interfaces) for VNF chaining, (b) “AI as a Service” tools and ML pipelines and (c) An open Data Lake of AI models and reusable training sets to be leveraged by vertical application developers. The Service Catalogue Repository will store the source code of Network Applications and AI pipelines, enabling its re-usability under open-source licencing as well as offering Distributed Version Control features. Furthermore, the Service Catalogue will implement a searchable index of reusable services, alongside their metadata and interfaces, integrating a Gitlab private repository solution. Thus, reusable assets will be searchable by 3rd parties that may implement Over the Top functionality that accesses Network Applications via their respective Northbound APIs or integrate AI SDKs and pre-trained models in their own applications. Finally, the Service Catalogue will provide a scalable file system for hosting the artifact files (e.g., Network Applications helm charts and container images, VNF images and descriptors, pre-trained AI models and training sets).

V. Testing as a service

FIDAL will deploy experimentation tools that target the media & PPDR industries and facilitate extensive testing of Network Applications and vertical applications via DevOps pipelines, that are considered the industry standard in modern production environments. Thus, testers and experimenters can seamlessly setup and execute FIDAL experimentation processes (e.g., unit and functional testing, continuous performance testing, validation/verification of KPIs) in a fully managed DevOps platform that supports “Testing as a Service”. The scope of FIDAL’s DevOps framework extends previous 5G projects, such as 5G-TANGO and 5G-MEDIA that mainly focused on the Development

¹⁸ <http://openslice.io>

processes, and offering emulators for service verification and 5GMediaHUB which focuses on the Operations processes of launched services, and specifically:

- Automated functional testing to verify their correct operation directly at the FIDAL infrastructure.
- Automated performance testing of newly deployed services, and validation/verification of their KPIs.
- Continuous validation/verification of service KPIs and adaptive, data driven QoE assurance.

FIDAL aims to offer a DevOps environment for 3rd party experimenters, which will hide the complexity of service deployment and testing and deliver a beyond 5G testing playground. Furthermore, it aims to deliver an adaptive, application aware NFVI that optimally serves the Media & PPDR industries, by promoting rapid prototyping via a Network Applications enablement layer and leveraging standardised solutions and interfaces that promote interoperability with other application domains.

The KPIs for FIDAL networks will need to be more advanced and comprehensive than the ones used for 5G networks. Here are the KPIs that are expected to be important for FIDAL networks:

Media Service KPIs (MSKPI) ¹⁹

1. MSKPI-01: App/Server Accessibility (%),
2. MSKPI-02: Content Load time/time to first picture (s),
3. MSKPI-03: Content Stall/Freeze (%),
4. MSKPI-04: Content Download Throughput (Gbps),
5. MSKPI-05: Content Upload Throughput (Gbps),
6. MSKPI-06: Application service creation (min),
7. MSKPI-07: Network Applications deployment time (min) Network Applications deployment time (min).

PPDR Service KPIs (PSKPI) ^{20 21}

1. PSKPI-01: Peak Throughput (Gbps/DL/UL),
2. PSKPI-02: Application latency (ms),
3. PSKPI-03: Positioning accuracy (meter),
4. PSKPI-04: User density (devices/m²),
5. PSKPI-05: Video resolution x fps x no of simultaneous videos,
6. PSKPI-06: Application service creation (min),
7. PSKPI-07: Network Applications deployment time (min).

2.4 UC methodology: KVI identification and associated process

FIDAL ambition is to adopt a consistent methodology to investigate the parameters that maximise 5G evolution service impact to the community. KVIs are designed to sit alongside KPIs to balance the Business and Social performance indicators. Such KVIs will be both evaluated through stakeholders' engagement in all trial phases as well as the open calls trials. Large scale electronic surveys targeting all EU countries and workshops with industry, academia and societal stakeholders will increase qualitative and quantitative analysis of the information leading KVIs evaluation and the respective proposals to maximise impact.

KVIs guide innovation as they aim to support systemic change to society's benefit by addressing societal challenges, pain-points, needs, and creating value for society. They provide a framework for considering the end-goal of innovation as a process — beyond the end-user's ability to use a tool or a system's ability to optimally function — to consider what

¹⁹ 5MS KPIs are defined in:

https://www.ngmn.org/wpcontent/uploads/Publications/2019/190111_NGMN_PreCommTrials_Framework_definition_v2_small.pdf.

²⁰ <https://tcca.info/documents/What-role-will-5G-play-for-critical-communications-users.pdf/>

²¹ <https://5g-ppp.eu/wp-content/uploads/2021/06/WhitePaper-6G-Europe.pdf>

is being changed or made better in society through the introduction of this innovation. They complement KPIs focus on the more immediate use with a focus on the broader impact an innovation has on the communities being served. This can range from values like addressing challenges such as engaging the last-mile or left-behind, to pain-points like societal distrust or a technology or service, or needs like upholding human rights, SDGs, and social justice concerns like equity. The objective of the KVIs process in the social issues that drive innovation uptake and sustainability. It is proactive and considers future consequences and impacts of proposed actions. It encourages innovators to engage in critical scrutiny and to think about social considerations to increase the reflexivity around definitions of “working” and “better”. It also engages stakeholders in ways that can affect the direction of a project from its earliest stages. Such understandings and evidence-base contribute towards the success of uptake, support the identification of stronger sustainability opportunities, and ensure increased stakeholder and public trust in the technologies and practices produced by FIDAL.

2.4.1 State of the art

I. 5G/6G specific frameworks from previous activities

a) HEXA-X results²²

Within the HEXA-X project (Deliverable D1.2 Expanded 6G vision, use cases and societal values), an early assessment of general social values was conducted to create an initial set of KVIs specific to 6G technology. These activities built upon the UN SDGs, but also looked more widely at other policy that defines social, economic, and environmental value. For this report, ‘value’ was defined as “intangible yet important human and societal needs such as growth, sustainability, trustworthiness, and inclusion” (p.61). It acknowledged that while some can be directly assessed, KVIs are most often assessed through proxies that are built upon a mix of qualitative and quantitative evidence. It identified as key values for the HEXA-X project (and thus aspects of beyond 5G, 6G):

- Sustainable 6G;
- 6G for sustainability;
- Inclusiveness & Acceptance (as a single value theme);
- Trustworthiness;
- Flexibility.

Sustainability here, in both directions in the list above, covers environmental, social, and economic aspects, and considers how to meet the needs of the present without compromising future generations’ ability to meet their needs. This requires considering the impact of the lifecycle of the solutions (e.g., technology and practices based in 5G, 6G) on sustainability (e.g., their impacts on environment, human rights, and socio-economic growth). It also requires considering how to develop the solutions as enablers of sustainability (e.g., their support for continued/flexible use, increased availability of good local jobs, changes in energy use practices, ability to better monitor climate change) over time.

The project has raised a few important challenges in relation to the application and evaluation of KVIs:

- **Quantifying values is much more difficult** than quantifying technical capabilities.

Implications for FIDAL: Tying the two together can be an option, where the KPIs are weighted in relation to a KVI.

- Technical performance can be treated in objective ways, whereas **values are often subjective or relational in nature** (grounded in situation, culture, scale, goals, ideology, regulatory framework, even organisational structure). Thus, any KVI framework needs to be able to adapt to different perceptions and backgrounds to identify the best indicators for purpose and context.

²² https://hexa-x.eu/wp-content/uploads/2023/05/Hexa-X_D3.3_v1.4.pdf; https://hexa-x.eu/wp-content/uploads/2022/03/Hexa-X_D1.3.pdf; https://hexa-x.eu/wp-content/uploads/2022/04/Hexa-X_D1.2_Edited.pdf

Implications for FIDAL: KVIs will likely neither be universal nor readily standardisable as abstract indicators, even if the value themes themselves are widely agreed upon.

- **KPIs and KVIs can lead to conflicting requirements.** As an example, provided, KPIs might seek to measure the global coverage of connectivity, which could include additional base stations and infrastructure, which in turn requires increased power consumption and could increase carbon footprint, contradicting KVIs that target decreased emissions and environmental harms.

Implications for FIDAL: While these do not need to be in conflict, abstract and isolated measures of both KVIs and KPIs could make them so. The relationships between these requirements need to be considered early and throughout a project to avoid trajectories that result in conflict.

- **Even when KVIs are quantifiable, interpreting them can be a challenge.** “Trustworthiness”, for example, can point to trust in a system, a person, a vendor, or a service. Indicators often necessitate multi-dimensional criteria. Similarly, interpretation requires careful definition of what elements/scale of a value is included. For example, is trust measured at a moment of use or along a supply chain?

Implications for FIDAL: **Indicators require multi-dimensions.** The necessary dimensions of indicators need to be clearly defined in advance with appropriate level of detail for shared interpretation. This means identifying the real questions being asked by an indicator and, very likely, seeking a series of indicators rather than one. However, the complexity of the value needs to be balanced with the practicalities of measurement in ways that provide real benefit.

b) *6G-IA White Paper on KVIs*

The paper, developed by the 6G Infrastructure Association Vision and Societal Challenges Working Group, Societal Needs and Value Creation Sub-Group, defines value as what is important to people and society that can be (partially) addressed or (indirectly) impacted by future network technology. Understanding value, thus, involves understanding the bigger picture (e.g., context, situation, ecosystem dynamics) to collaboratively, with stakeholders, identify the greater good being worked towards. This, the WG notes, requires a mindset shift and reframing, driving innovation not only with technological specifications and business values but thinking more broadly about the implications for society (and all the nuances within). A societal value-based approach requires asking questions like “**what does this enable within or give to individuals, communities, society**”?

KVIs are intended to complement a more traditional performance based (KPI) approach and serve to (a) demonstrate the validity of innovation towards meeting societal needs, and (b) impact innovation trajectories towards benefiting values (in addition to user needs). It is used to formulate targets that are measurable (quantitatively “number of users a service fulfils” or qualitatively “perception of value fulfilment of using a service). The end goal is to develop a mechanism to empirically demonstrate how an innovation brings that value. They are described along with **enablers**, that support reaching the targets.

Building upon the societal values engaged within the UN SDGs, the European Green Deal, Human-centred design, as well as the broader European values of strategic autonomy and technological sovereignty, the WG suggest Key Value Themes from which 5G/6G use-case-based indicators can be built:

- Environmental sustainability;
- Societal sustainability;
- Economic sustainability and innovation;
- Democracy;
- Cultural connection;
- Knowledge;
- Privacy and confidentiality;
- Simplified life;
- Personal freedom;
- Personal health and protection from harm;

- Trust.

They further propose that an indicator developed should support assessment pathways, that include (in various combinations):

- Objective evaluation by experts and representatives: expert assessments, measurements taken from the deployed networks themselves.
- Subjective evaluation by representatives: data gathered from trials, experiments, interviews, questionnaires, focus groups.

They provide a 4-step pathway to KVI formulation:

1. Define the KVs relevant for the use case. This is tied with building an understanding of the relevant “pain points” or broader societal challenges being faced that drive the value.
2. Identify the KVI. This should be done via assessing the scale of effect (e.g., by asking what part of a population realistically is affected through a use case?).
3. Determine enablers and blockers. These are both technical and social and involve asking questions like: what would make the use case popular? What would limit availability? What key factors support/limit scaling up?
4. Quantify (when possible) indicators with KPIs of their own. These can be technical or numerical targets that (according to expert stakeholder assessment) enable KVs. Any KPI should be described such that it is clear how and to what extent it represents an improvement towards a KPI.

The WG also raises some key points regarding KVIs that are relevant to the development of the FIDAL KVI methodology:

- **Project and use case goals must be clarified prior to formulating metrics.** Goals here, must be beyond technical achievements but build in an understanding of the context in which a technology is put to use, and how it is used. This requires input from diverse stakeholders relevant to those contexts (e.g., social scientists, natural scientists, practitioners, community representatives, local businesses).

Implications for FIDAL: while it is possible to develop higher-level preliminary KVIs at this stage, specific KVIs should be developed alongside the finalisation of the project use cases.

- KVI formulation, assessment, and causality towards a value should **involve relevant experts and stakeholders**. In part, this is needed because causal chains from measures to impact are not straightforward nor within project timeframes. This is particularly important in order to avoid unintentional inflation of value terms or “value-washing” (in lines of green-washing or ethics-washing).

Implications for FIDAL: KVs and KVIs should be co-developed and co-evaluated with relevant stakeholders for the use-cases.

- **KVIs are always only a demonstration of potential value** but not directions/instructions for how to design for impactful technology.

Implications for FIDAL: Key values are the enablers that should impact solution and use case design, and from these KVIs should be treated only as proxies to know if we are pointed in the right direction. Completion of KPIs should not be conflated with achieving a value.

II. General Social Value Frameworks

a. EU's Taxonomy Regulation ²³

The EU's regulation that establishes an ESG Taxonomy provides a strong legal basis and classification system for defining indicators, as it is designed to encourage standardisation, comparability, and transparency of sustainability measures across a range of environment, societal, and governance objectives, including (among others):

- **climate mitigation:** “contribute substantially to the stabilisation of greenhouse gas emissions by avoiding or reducing them or by enhancing greenhouse gas removals” (para 24)).
- **climate adaptation:** “contribute substantially to reducing or preventing the adverse impact of the current or expected future climate, or the risks of such adverse impact, whether on that activity itself or on people, nature or assets” (para 25).
- **circular economy:** “increase the durability, reparability, upgradability and reusability of products, or can reduce the use of resources through the design and choice of materials, facilitating repurposing, disassembly and deconstruction in the buildings and construction sector, in particular to reduce the use of building materials and promote the reuse of building materials” and “by developing ‘product-as-a-service’ business models and circular value chains” (para 28).

The aim of the legislation is to harmonise the criteria for determining whether an economic activity qualifies and environmentally sustainable. It further supports the obligation to disclose how and to what extent the criteria is used in ways that are understandable to others. For each objective, the legislation presents a series of pre-indicators, defining their scope and offering guidance that FIDAL can draw upon for its KVs. For instance, for climate change mitigation it looks for instruments that use renewable energy, improve energy efficiency, switch to the use of sustainable materials, and do not hamper the development and deployment of a low-carbon alternative (e.g., does not lead to lock-in of current emissions).

b. OECD's guidance on including societal values in public procurement²⁴.

The OECD acknowledges the power behind the choice of technologies/solutions governments and businesses make and purchase) to be a strategic policy lever for governments. Technologies/solutions that help governments meet policy objectives can contribute directly to public goods (e.g., trust, well-being, prosperity, inclusive societies). Anticipating future challenges and focusing innovation (and investment in that innovation) in these spaces can be one way to support meeting societal needs. It notes that seeking technical specifications/solutions in isolation of the policy objectives will likely lead to results that, while cheaper than existing solutions, will more likely produce results that are “less innovative but still within the minimum requirements” (p. 15). Taking green policy as an example, they note that while on the surface a solution might seem cheaper, considering the “hidden costs” that come with stable or increased emissions and e-waste, a different product could be cheaper across a product's lifecycle. While primarily focused on public procurement of innovative technologies, it describes key principles -- and provides a series of indicators for them -- that have been demonstrated to connect innovation to societal values and good public policy. Most relevant to FIDAL are:

- **Social Impact:** including improved economic results, greater inclusivity for vulnerable and marginalised groups in the growth experienced, prioritising wellbeing, gender equality, job creation, and considerations of human rights.

²³ REGULATION (EU) 2020/852 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 18 June 2020 on the establishment of a framework to facilitate sustainable investment and amending Regulation. Available at: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32020R0852&from=EN>; https://finance.ec.europa.eu/sustainable-finance/tools-and-standards/eu-taxonomy-sustainable-activities_en#what.

²⁴ OECD (2019). Report on the Implementation of the Recommendation of the Council on Public Procurement. C(2019)94/FINAL. JT03449826. Available at: [https://one.oecd.org/document/C\(2019\)94/FINAL/en/pdf](https://one.oecd.org/document/C(2019)94/FINAL/en/pdf)

- **Environmental Impact:** considering the lifecycle in the cost-benefit assessment, use environmental standards in decisions around materials, recycled content, and production methods, as well as awareness raising.
- **Transparency:** sharing processes to support public scrutiny and free access, to the extent possible while considering IPR, trade secrets, security, and related liabilities. The aim should be to level the playing field by fostering accountability, ensuring access to information, and enabling participation of diverse stakeholders.
- **Integrity:** often represented by codes of ethics, standards of conduct, and safeguard mechanisms, it is critical in strengthening governance and building resilience. It is fostered most when clear rules are outlined that build on key principles such as equal treatment, non-discrimination, transparency, proportionality, and effective competition.
- **Access:** this is guided by inclusivity and non-discrimination. It has been measured in the past by including requirements for minimum percentages of societally marginalised groups or by offering percentages of opportunities to these communities.
- **Risk Management:** this can include development of risk matrices/maps and controls along with monitoring mechanisms with timelines and consequences. Important to this, according to the OECD is the public reporting of these risks (to the extent reasonably possible).
- **Accountability:** provided through oversight and control mechanisms, with clear chains of responsibility. This includes a risk management process.

It notes two common ways to measuring societal value, both like more traditional performance measurement practices. One can benchmark, for example by comparing one's own operation with a similar one. One can also compare monitoring indicators against pre-defined performance targets (that are relevant, attributable, well-defined, timely, reliable, comparable, and verifiable). Indicators can include both elements of a system/process (e.g., % of overall system/processes) as well as stakeholder perceptions of the system/process (e.g., surveys).

c. UK's Social Value Act and Implementation ²⁵

While outside the EU, but still within Europe, the UK's Social Value Act from 2012 (economic, social environmental) is a unique legal articulation of a model for defining and assessing social value that has been applied at the local council level. It is specifically designed to support the evaluation of social values in tenders for the public sector. To support, guidance has been created in the form of the National TOMs Framework (TOM, Themes Outcomes, and Measures) to support minimum reporting standards to justify social value outcomes. It builds upon the policy objectives of the SDGs and offers criteria for evaluation that supports measuring what has been done and also the potential to deliver a broader impact. Relevant social value themes include:

- **Promoting Skills and Employment:** grow and develop opportunities (with access for all) to develop new skills and gain meaningful employment. (e.g., via delivery of training schemes, literacy support, safety talks, traineeships).
- **Creating Healthier, Safer and More Resilient Communities:** build and improve relationships with organisations to empower citizens. (e.g., via involvement of diverse communities in design, community led initiatives, reducing loneliness, reducing crime, meaningful social mixing).
- **Protecting and Improving our Environment:** ensure cleaner and greener places, to secure the long-term future of people and planet. (e.g., working towards net-zero emissions, managing, and reducing environmental impacts along the supply chain and throughout the life cycle including future maintenance).
- **Promoting Social and Disruptive Innovation:** find innovative solutions and new ideas to old problems. (e.g., via outcome-based innovation that enables an alternative approach, promote collaboration, future-proofed).

These are defined with additional details to other frameworks presented here that support clarity and shared understanding. Categories include:

- **Value:** overarching objective.
- **Theme:** specific objective within.

²⁵ https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/940826/Social-Value-Model-Edn-1.1-3-Dec-20.pdf;

- **Type:** input to activity, output of activity, outcome of activity, impact of activity.
- **Value for who:** who directly benefits from the indicators, focusing on individual, community, and government.
- **Indicator:** how will you measure this.
- **Unit of measure:** how it should be recorded for measurement.
- **Evidence:** what will provide the evidence for the measure.
- **Rationale:** description of why and how this shows a value trajectory, even if just pointing towards a longer-term impact the indicator is only a component of or yet to be achieved.

As part of this, a National Themes, Outcomes and Measures (TOMs) framework was developed by the Social Value Portal to support development and identification of KPIs that measure and report social value. Drawing ²⁶ examples from it can improve the richness and validity of the KVI's developed in FIDAL. Two examples from their TOMs are below:

KV: Social value embedded in the supply chain

KVI: % of contracts with the supply chain on which Social Value commitments measurement and monitoring are required.

(Y/N) existence of requirements on businesses operating in the local area to create, monitor and measure social value.

Evidence: via record of relevant contracts.

KV: Savings in CO2 emissions on contract not from transport which could result from a deliberate programme aimed at changing industrial processes.

KVI: More use of sustainable energy sources in local industrial processes and business operations (e.g., Renewable Energy) (YES/NO).

Evidence: Through an independent and verifiable process (e.g., Planet Mark Certification or equivalent).

d. The Wales Well-being of Future Generations Act ²⁶

Similarly, the Wales Well-Being of the Future Generations Act of 2015 creates a legal requirement to think about the impact of activities on future generations (e.g., poverty, climate change, health inequalities). It acknowledges that sustainable development involves more than just single category focus (e.g., engaging emissions or economics alone) but all aspects that support individual and community well-being. It is intended to encourage longer-term impact awareness and planning to be a balance (and in conversation with) shorter term performance measures. It legally requires public bodies and businesses to:

- impact all the well-being goals,
- show that the indicators make a complete set,
- show they are aware of how their indicators affect others, and
- justify the indicators as appropriate.
-

It defines sustainable development through seven goals, with an indicator framework to support measuring them qualitatively and quantitatively. Relevant to FIDAL are:

- **Prosperous:** innovative, productive, low carbon society which uses resources in ways that acknowledges their limited nature. It also develops jobs and education. Potential indicator from Act: innovative businesses, productivity, renewable energy, people in work, adults with qualifications.
- **Resilient:** maintains biodiversity and healthy functioning ecosystem that support economic and ecological resilience. Potential indicator from Act: air quality, waste not recycled, people satisfied with where they live,

²⁶ <https://www.gov.wales/sites/default/files/publications/2021-10/well-being-future-generations-wales-act-2015-the-essentials-2021.pdf>; <https://www.gov.wales/well-being-future-generations-wales-act-2015-guidance>; <https://www.gov.wales/wellbeing-wales-national-indicators>

social value partnerships, energy efficiency of homes, hazard free homes, sense of community, healthy ecosystems.

- **Healthier:** people's physical and mental well-being is maximised. Potential indicator from Act: Healthy lifestyle, Satisfaction with access to facilities and services, feeling safe, greenhouse gas emissions.
- **More Equal:** people can fulfil their potential no matter what their background or circumstances. Potential indicator from Act: adults with qualifications, fair pay, people living in poverty, people with access to services, loneliness, young children developing the right skills.
- **Cohesive Communities:** communities that are attractive to live in, safe, within reach, and well-connected. Potential indicator from Act: People feeling involved, participation in culture and heritage, volunteering, sense of community, feeling safe.
- **Globally Responsible:** considers how acts inside the country affect those outside. Potential indicator from Act: air quality, greenhouse gas emissions, healthy ecosystems, energy efficiency of homes, people living in poverty, global footprint, renewable energy, innovative businesses.

These have been translated into a series of annual indicators, targets, and milestones. Guidance **Error! Bookmark not defined.** published in relation to the Act offers a framework for initial social value assessment, to better understand baselines to measure from and ways to identify where to most effectively contribute to [6]:

Table 4: Guidelines understanding your contribution.²⁷

Identify the functions that you exercise that best contribute to all of the well-being goals: What is our purpose and what are our current functions and duties?
Understand your current contribution: Where do we currently make a contribution? Are there well-being goals that we contribute more to, than others?
Understand your potential contribution: What more could we do? What could we do differently to make a better contribution? Are there things we should do less of, or stop doing?
Identify the opportunities for maximising your contribution (making a greater contribution): How do we turn our potential contribution into action through the well-being objectives we set and the steps we take? What could we do that would enable others to contribute more?

2.4.2 Key Values and Indicator Framework

Together, this previous research, regulation, and application offers a high-level framework for FIDAL's indicators. These are presented with example indicators (measures). Which of these are relevant is to be determined in consultation with stakeholders in the contexts of the use case development, as goals are solidified.

I. Democracy

Trustworthy: Solution deemed trustworthy; stakeholders trust fellow users/governance; trustworthy infrastructures and networks, trusting of other users, public trust in systems and authorities, trust in a behaviour or process, trust in institution. Can be broken down to confidence, integrity, consistency, commitment, accountability, control mutuality, exchange relationships.

Table 5: KVs and Trustworthy.

Trustworthy	Dependability	100% stakeholders deem system dependable for their activities
	Consistency	100% consistent coverage of the network
		Comparison of latency of data transmissions (previous vs current)

²⁷ <https://www.gov.wales/sites/default/files/publications/2019-02/spsf-1-core-guidance.PDF>

		Probability of error; ease identification of error
		0% potential bias detected
	Building confidence	Survey responses on reported confidence in advanced digital devices, systems, and services in critical missions and media, from different segments of society, including both general public and users

Inclusiveness / Equal Opportunity: Able to support a range of existing community devices, giving service access to the widest possible range of demographics in a community. Serve the historically under-served; consider broader demographics and ensure they are included in the benefit from the innovation. This include both social and digital inclusion, reducing the digital divide of who has access.

Table 6: KVs and Inclusiveness.

Inclusiveness	Service Availability	Up to 99.9% communication service reliability
	Service Access	Ratio, Increased community access to use services, across all demographics as defined by community authorities
	Embedded devices	Comparison, Increased embedded devices from historical numbers
	Local Skills Creation	# of trainings offered to marginalised groups

Fairness: Impartial and just treatment without discrimination. Outcomes of decisions aimed at avoiding disparate effects on different groups, unless relevant differences cause uneven benefit or burden. What is fair for a group might conceal unfairness for individuals. Neutrality and equality are not always equivalent to fairness.

Table 7: KVs Fairness.

Fairness	Access to participate in decision-making	Survey on access to active participation in relevant administrative and political functions regarding 5G and solutions.
	Lack of Bias	Ability to evaluate for bias in algorithms/systems being produced (using stakeholder definitions of bias).

Personal freedom: Related to flexibility, programmability, autonomy, and dignity.

Table 8: KVs and Personal Freedom.

Personal Freedom	Ability to make decision/human-in-the-loop	Survey on user perception of system programmability, control
		% of decisions made by tools with human supervision
	Dignity	Survey of users and stakeholder perceptions of the impact of tools on their personal dignity.

Transparency: Understandability, ability to justify to others, ability to explain how fit within goals; public facing when appropriate/possible for accountability.

Table 9: KVs and Transparency.

Transparency	Auditability	100% ability to trace actions taken with data, processes
		% of processes that support public scrutiny (that are not security sensitive)
	Understandability	Survey, user perception of intentions, purposes, and goals of technology and processes, access to information

	Justifiability	Survey, users' ability to justify the use of a solution to others, including the public
	Explainability	Survey, users correct assessment and instruction around the technology and processes, including specific questions that demonstrate literacy

Privacy: Confidentiality in of the person (communication, movements, interactions, etc.)

Table 10: KVI and Privacy.

Privacy	Privacy preserving	100% privacy concerns of users addressed (defining access rights, appropriate policy, user ability to control and define)
----------------	---------------------------	--

II. Economic Ecosystem (part of sustainable 6G)

Economic Sustainability: Pointing towards a prosperous and ethical economy. Building a competitive and resilient EU economy, investing in jobs, skills, education, and digital transformation.

Table 11: KVI and Economic Sustainability.

Economic Sustainability	Businesses in or with access to supply chain	Number of stakeholders added, contacted, or considered for design and production; Diversity of those businesses engaged.
	Market impact	Reduced risk of becoming stranded as a result of transitions reduced
		Increased market space for each tool (% of total market, number of sub-markets, relative customer reach)
	Supply chain sustainability	% of supply chain elements traced of total supply chain
	Improved productivity and effectiveness	Survey of stakeholder perspectives on their productivity and effectiveness of their activities
	Engaging legacy systems	% pre-existing systems that require modification to be employed in use-cases
	Resource Savings	Quantity of resources saved (money, time, material) predicted through the use of the tools
Use of whole of life costing	Ratio, value, and number of assessments following a procedure containing life-cycle costing award criteria	

Business Value: Inclusive commercial benefit, maintaining and building new market spaces, developing new value chains.

Table 12: KVI and Business Value.

Business Value	Solve existing and emerging problems	Survey, stakeholder perceptions of problems solved (fully or partially)
	Production of business plans	Production of at least 3 business plans. Production of at least 10 individual plans
	Cost and time to engage with services	Survey of users, including quantitative results, on time taken and resources engaged in use-cases
	Supplier concentration	Ratio of suppliers from different groups (e.g. large industry, SMEs, women-owned, etc.)

Tackling economic inequality: Creating new business opportunities, increase supply chain resilience and capacity.

Table 13: KVI and Tackling economic inequality.

Tackling economic inequality	Decrease Cost	% cost decreased for access components, connectivity, system as a whole.
		% cost saved by working with such solutions over defined period of time.
	Training opportunities	Number of training opportunities, local school visits, curriculum and literacy support, safety talks, etc., supported and expected to be completed
	Improved local business opportunity	Survey, local businesses that see the use-cases as opportunities they could engage with
	Output relevant to multiple socio-economic demographics	Survey, diverse stakeholders' perceptions of relevancy and value of use-case outputs

III. Innovation

Responsibility: Being accountable for (and having control over) system behaviours.

Table 14: KVI and Responsibility.

Responsibility	Accountability	Existence and effectiveness of risk management oversight and control mechanisms, with clear chains of responsibility
	Enables alternative approaches	Number of alternative approaches possible for each system configuration
	User Control	Ratio of system behaviours users can manipulate

Open collaboration: Using methods based on collaboration and knowledge sharing. Include end-users and stakeholders in processes. Work through co-design with local/stakeholder organisations.

Table 15: KVI and Open collaboration.

Open collaboration	Awareness	Survey, Improved awareness among partners and users of stakeholder values, challenges, and needs.
	Participatory processes/methods for community engagement	% of services developed with users and suppliers both integral to the design
		Survey, effectiveness of methods
		Number of end-users and stakeholders included in design and testing process, number of opportunities for participation for each one.
	Community networks	Increase in community networks (% increase, number total).

Flexibility: Ability to work in multiple situations, contexts, goals, configurations.

Table 16: KVI and Flexibility.

Flexibility	Optimal resource allocation	100% ability to reallocate resources if local system failure. Flexible resource allocation and redistribution of functionality can increase the system robustness and flexibility in the direction of succeeding sustainable coverage
--------------------	------------------------------------	--

	Re-use/re-purpose of existing devices and infrastructure	% integration and utilisation of existing devices, networks, and services, supporting the long lifetime of industrial equipment and flexibility of service growth. (Coexistence of Non-3GPP and 3GPP networks)
	Ability of AI models to adapt to different conditions	100% Flexibility to deploy same system in multiple scenarios without many modifications, in timely fashion
	Data economy	Range of quantity of data needed. Capability of achieving high inferencing accuracy with a smaller amount of learning data.

IV. Environmental Ecosystem (part of 6G for sustainability)

Environmental Sustainability: To reduce its footprint on energy, resources, and emissions and improve sustainability in other parts of society and industry.

Table 17: KVs and Environmental Sustainability.

Environmental Sustainability	Reduction in Energy Consumption	~100% device energy efficiency
		0% energy efficiency degradation due to activity
		% improved energy efficiency compared to current status
	Air Pollution Reduced	% improvement in route or system efficiency
	uses renewable energy	% energy from renewable resources
	Reduced Environmental footprint	reducing the use of primary raw materials or increasing the use of by-products and secondary raw materials
		does not hamper the development and deployment of a low-carbon alternative (e.g. does not lead to lock-in of current emissions)
Decreased virgin resources used over a product lifecycle	Physical/ earth resources savings as percentage of current consumption in specific, locally and timely defined context.	

Waste Management: Reduce, Re-use, Recycle materials, emissions, life-cycle impact, infrastructures.

Table 18: KVs and Waste Management.

Waste Management	Reduced Waste through recycling or repurposing	100% of devices - recycled
		100% of sensor devices' usage checked.
		~100% reuse of existing equipment
		~0 additional deployments
		Reduced waste in supply chains
	Increases Lifespan	Increased the durability
		Increased reparability, upgradability, or reusability of products
Ability to assess the production, use and end of life of products and services		

Mitigation Strategies: Demonstrate awareness of environmental impact with a strategy to minimise it (or increase actions on it).

Table 19: KVIs and Mitigation Strategies.

Mitigation Strategies	Greater understanding of environmental challenges	Number of environmental factors monitored for (of air quality, garbage flows, traffic, emissions, etc.)
------------------------------	--	--

Compliance Quality Standards: Engage environmental quality standards, even if not regulation.

Table 20: KVIs and Compliance Quality Standards.

Compliance Quality Standards	Energy efficient low EMF exposure network operations	EMF measured below health concern quantities
	Decrease Hazardous Content	reduces the content of hazardous substances and substances of very high concern
	Union labelling and certification schemes for assessing environmental footprint	% of project outputs based on such certifications and related methods.

V. Safety and Security

Safety: Protection of humans, to prevent harm, safer communities.

Table 21: KVIs and Safety.

Safety	Risk Management	Development of risk matrices/maps and controls along with monitoring mechanisms with timelines and consequences. Important to this, according to the OECD, is the public reporting of these risks (to the extent reasonably possible).
	Feeling safe	Survey, user and stakeholder perception of personal and community safety resulting from tool use.
	Easy to use tools	Survey, users find tools easy and self-explanatory
	Vulnerable people have greater protection	Increase in vulnerable populations served (number of demographics able to be reached, population spread, geographic spread)
	Increased operational efficiency for saving lives in emergencies	TBD by end-users.
	Reduced injuries in PPDR missions	% of actions taken with a device (before vs after) that suggest decrease risk taken by first responders.
	Hazards are reduced	TBD by end-users.

Security: Protection of data and socio-technical systems in a way that prevents negative impact.

Table 22: KVIs and Security.

Security	Vulnerabilities	Ratio of vulnerabilities identified and fixed to safeguard FIDAL's users.
	Delegation	Number of processes that delegate responsibility to appropriate parties and ask them to consider their impact to the wider ecosystem.
	Security preserving	100% system secured

Data protection e.g., the appropriate use of personal data.

Table 23: KVIs and Data Protection.

Data Protection	Personal Data Protected	100% personal data protected from unauthorised use. 100% of providers/services have accountability mechanism in place (both technological and organisational)
	User Control	100% user control over personal <i>data for storage/transmission/processing (as appropriate to rights)</i>

VI. Societal Ecosystem (part of 6G for sustainability)

Societal sustainability: Guide/support convergence of physical, human, and digital worlds.

Table 24: KVIs and Societal sustainability.

Societal sustainability	Representation in use-cases	Use-cases that reflect the diversity of local communities they should benefit; reflect urban and rural opportunities Steps taken to have outputs that are relevant and can reach stakeholders (across age, race, gender, region); number of activities that can be done anywhere.
	Stakeholder perception and involvement	Survey responses from different segments of society (e.g., businesses, civil society, NGOs)
	Prioritising wellbeing	Ratio of design decisions made that prioritise well-being.
	Gender equality	Ratio (from survey) of project outputs deemed relevant and useful for men and women.
	Individual cost savings	Average cost saving per person

Healthier community: Making communities more desirable and better places to live; improve the bodily and mental health of individuals.

Table 25: KVIs and Healthier community.

Healthier community	Build and improve relationships with organisations to empower citizens	Number of opportunities (and people) for involvement of diverse communities in design, community led-initiatives, reducing loneliness, reducing crime, meaningful social mixing.
	People satisfied with where they live	Survey, satisfaction with access to facilities and services

Cultural connection: *Inclusive cities*, emerging socio-technical networks, diversity, arts, heritage, and knowledge systems.

Table 26: KVIs and Cultural connection.

Cultural connection	Access to cultural products	#products / product types by who
	Access to cultural events	(#events / product types by who)
	sense of community	Survey, people feeling involved, participation in culture and heritage
	Cultural Domains	Number of cultural domains impacted

Knowledge: Enhance technical skills and empower researchers and industrial players with new digital skills.

Table 27: KVIs and Knowledge.

Knowledge	Enhanced Technical and Research Skills	# of trainings offered to researchers or industry players
	Access to knowledge	Number of people with access to quality education (at all levels, esp. higher); Access to digital libraries; Access to and interaction with knowledge groups
	Improved public digital literacy	Survey, stakeholder understanding of issues raised by FIDAL

Quality of Living / Wellbeing

Table 28: KVIs and Quality of Living.

Quality of Living	Improving Wellbeing	% staff content with jobs
		% of persons content with community

2.4.3 KVI Methodology

KVI mapping requires a multi-step process.

a. Identify stakeholders and articulate challenges, pain-points, and needs.

We will work in collaboration with end-users and solution developers, as well as with broader stakeholders and subject-matter experts. These interactions will be via small-scale workshops, interviews, and focus groups, starting at the local level of the use cases (e.g., 1-2 interviews or focus groups per use-case). As the project moves towards looking at the EU-level, these will be complemented by larger workshops/focus groups and interviews. These interactions will aim to:

- Identify key stakeholders for the project and what actions are in their best interests.
- Understand how the project meets its objectives to identify relevant values. This will be done by mapping the **problem-solution definition** of the project.
- Identify the broader societal **pain-points around 6G and the values gained** from having them solved. As part of this, we try to articulate what is innovative (e.g., not the newest gadget, but what societal systems change).
- Agree upon outcomes, as relevant for context.

b. Identify relevant values with positive impact towards the use cases.

As value is not derived from a tool itself (a knife is neither beneficial nor harmful on its own, only in use), the use-cases and stakeholders will drive the value mapping process. The best interests are key in deciding what outcomes should be the focus of the value strategy.

- Map and assess the use cases to understand the use contexts that inform **what is at stake for who** and thus which values take priority.

c. Define scale and scope for the values.

This includes identifying the KVI itself. This will be done through co-design processes to:

- Identify **measures on how successful or widespread** a value might be (e.g., individual, community, regional, national). These measures could change depending on who gains the value or the size/impact on the population.
- Identify **what part of the solution and use cases is relevant** for each value. For example, does that scope speak to the technology being developed, the infrastructures, a procedure, training or knowledge transfer, user

and/or public literacy, or policy changes. This will help with **attributions of responsibility towards KPIs** and ensure indicators match tools potential.

d. **Identify enablers and blockers.**

For example, what elements of the technology being developed could support achieving an impact (even if only one small part of the larger value puzzle). For example, trust can be enabled by system auditability, rugged and robust devices; Secure and trustworthy AI; System E2E privacy and security. Or, feelings of safety can be enabled through joint communication and sensing, easy to use devices; Network and service automation.

- What key factors in the project (and beyond the scope of the project, such as new practices or policies) can enable or limit the KVs?

e. **Assess how the indicators relate to project timing.**

- Project development stages;
- Key points of assessment;
- Points of rigidity/conclusion (where design or practice can no longer change).

f. **Define measures of success**

From this, we will:

- Articulate an initial list of values the project wants to uphold;
- Articulate why those values;
- Suggest who will benefit;
- Quantify and quality the KVs with KPIs of their own.

These steps will be revisited, iteratively throughout the project. The resulting KVs and KPIs will be stored in a **repository**, mapping the interrelationships and dependencies between the steps and the project components. A draft repository structure is in the figure below.

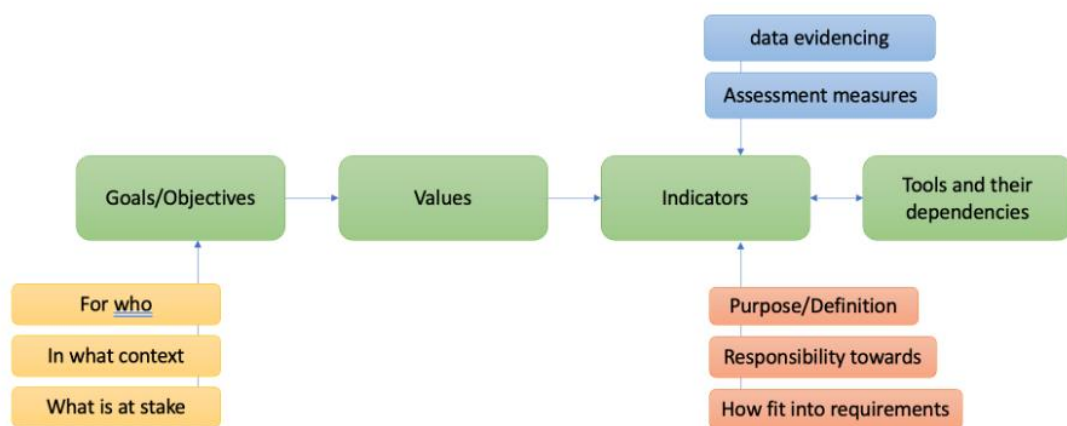


Figure 4: FIDAL Repository structure.

g. **Evaluation**

The KPIs will be both evaluated through stakeholders' engagement in all trial phases as well as the open calls trials. Large scale electronic surveys targeting all EU countries and workshops with industry, academia and societal stakeholders will increase qualitative and quantitative analysis of the information leading KPIs evaluation and the respective proposals to maximize impact. This will need to involve outputs directly derived from the use-cases, both stakeholders involved directly in the use-cases, broader stakeholders (e.g., relevant community members), as well as the partners involved in the project (e.g., mapping their business practices). The evaluation process will:

- A. Assess current status of measures and targets;
- B. Inform necessary modifications or continuations to reach targets;
- C. Support in evaluating less straightforward questions around proportionality, such as how to make the case that greater cost (thus a lower KPI) can create greater equity in access (thus higher KVI)?

2.5 UC methodology: Testing, experimentation, and validation of KPIs and KVIs 28 29

While this document can be seen as a very early iteration of FIDAL technologies, this methodology will be used while evolving the UCs and the subsequent testing, experimentation, and validation cycles. These cycles and updates will be further reflected in the updated deliverable D2.2. According to A, B and Nesse et. al [2] an agile development process is recommended as best practice for 5G research and innovations (R&I) projects (see Figure 5: Agile development methodology and validating of KPIs and KVIs. This backdrop of this process is the work of Cooper [3] [4] through his iterative, agile, and open innovation modifications of the original stage-gate model. Moreover, still [5], suggesting a similar methodology for R&I activities for universities and other public research institutes, mitigating the high degree of failure in translating scientific advances into marketable innovations.

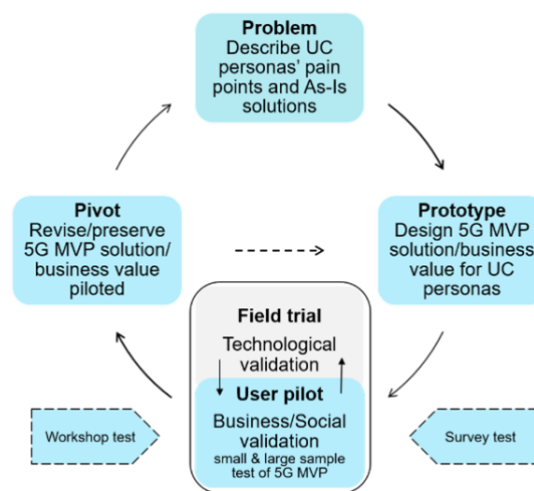


Figure 5: Agile development methodology and validating of KPIs and KVIs.

- **Problem:** Here the use case problem and personas/stakeholders are described: Description of as-is situation and current technology solutions in use by stakeholders was also included. Design thinking and empathy mapping visualize customer types/personas and pain points, and customer journeys adds to the understanding of the customers interactions (touchpoints) with consortium partners.
- **Prototype:** A prototype/minimum viable product (MVP) is designed as a solution that mitigates the personas' needs and pain points revealed at the prior stage. Protocepts³⁰ in the form of information material and videos are designed with the purpose to describe and visualize the 5G use case MVP's.
- **Pilot/trial:** Here technical trials of the MVP's are performed, typically validating the 5G network requirements (KPI's) such as latency, coverage, data/speed, and reliability. Simultaneously, business and consumer pilots of the 5G protocept/MVP with relevant use case stakeholders can also be performed, validating KVI's such as user experience (QoE), revenue increase, digital inclusion and reduces energy consumption. This will demand

²⁸ A 5G PPP, "Business Validation in 5G PPP vertical use cases," 2020d. 5G_White_paper_Business-validation-v1.0a.pdf (5g-ppp.eu)

²⁹ 5G-SOLUTIONS, "D1.4A Methodologies for the validation of 5G, 2019. Deliverable-D1.4A-Methodologies-for-the-validation-of-5G-and-for-LL-measurements-v1-WIT-Final.pdf (5gsolutionsproject.eu)

³⁰ This is a short notation for the information material and videos describing the MVP / prototype. Infographics might be one kind of relevant information material.

a different methodology, e.g., physical or virtual focus groups/workshops with 20+ stakeholder personas facilitated by a moderator followed up with an online survey for a larger sample of potential stakeholders.

- **Pivot:** The findings from small and large sample pilot tests are aligned with results from technology validation field tests. One outcome is that to move ahead with the MVP solution (“persevere”). Alternatively, a modification of the solution design and specifications is necessary (“pivot”). In the latter case, it is necessary to return to start if the problem and pain points are understood and thereafter proceed to redesigning the prototype, hence the dotted arrow [2].

Briguglio et. al [6] suggest a combination of business and social context variables when validating 5G related R&I outputs. These variables (KVI's) and inspired from 3GPPP white paper on social impact³¹ Nesse et. al [2] recommends simultaneous validation of business value, social acceptance, and technology performance in 5GPPP R&I projects. This should start already from the initial trials (iteration #1) using minimum viable products (MVP), protocepts or other simple sketches etc. to provide precise and high value feedback from potential stakeholders for further modifications. Moreover, the three impact dimension groups should be validated equally important. The background is an agile development methodology when developing early MVPs secures the process of learning as quickly as possible to get a desirable product to customers' hands faster [7].

While anticipating the above high-level methodology FIDAL will further detail, adapt and develop the relevant methodologies and the (use of) supporting tools for such joint technological and business validation suitable for the FIDAL UCs. The references above (footnotes 29, 30 above) can be seen as the baseline for the testing, experimentation and validation methodologies and report formats.

A critical step in this process is the staging and on-boarding of UC and test-case (TC) specific VNFs/CNFs in addition to any 5G network specific on-boarding, setup and configuration. This can imply the setup of a new 5G network slice or merely adapting and configuring an existing 5G network slice according to the needs of the UC and the TCs. This topic and related methodology are described in Section 15.

³¹ 6G Infrastructure Association, "What societal values will 6G address? Societal Key Values and Key Value Indicators analysed through 6G use cases," May 2022. [Online]. Available: <https://5g-ppp.eu/wp-content/uploads/2022/05/What-societal-values-will-6G-address-White-Paper-v1.0-final.pdf>

3 Use Case analysis overview

The previous chapter detailed the adopted methodology for providing a clear and complete analysis of the use cases, describing the process to examine the technical and business aspects for each UC. This section provides an initial concise analysis and overview of the use cases, providing some essential information about the scope and the market value of each use case.

3.1 Market assessment, analysis, and feedback

3.1.1 Media vertical industries assessment

Media are required to closely follow and adopt new technologies, especially in high-speed connectivity in order to stay competitive in a highly fragmented market. Proliferation of Evolved 5G technologies is bound to facilitate expansive growth in live video streaming. The IBM Institute for Business Value (IBV) 2019 Global Telecom and Media Consumer Survey confirms the trend for 5G in 21 countries worldwide, indicating ultra-high definition (UHD) as by far the most relevant 5G application. Evolved 5G is expected to unlock further the potential of immersive applications in Live TV broadcasts and sporting events (e.g., AR/VR), which are forecast to create more over \$140 billion in cumulative revenues by 2028.

FIDAL will leverage Evolved 5G experimentation infrastructure deployments to deliver a promise for increased bandwidth and low latency, thus accelerating development prototyping and growth for novel mobile video technologies and streaming services, representing a major opportunity for European SMEs to reduce the barrier to market penetration and hence enable the EU to stay competitive in the global Media market.

3.1.2 PPDR vertical market assessment

According to Mordor Intelligence, a \$11,15bn public safety market is expected to grow almost fivefold within the next 5 years, at a CAGR of ~30%. Cloud deployments are expected to account for the largest share of this growth, due to expenditure cuts on budgets forcing public safety providers to forego investments in infrastructure in favour of Cloud-based solutions. New technology solutions in this segment (including e.g., geographic info, simulation and surveillance systems) are expected to surface as a result, being absorbed by both the public and private sectors as a means to anticipate, react and mitigate the effects of natural and anthropogenic hazards. To this end, 5G-enabled URLLC apps play a significant part in the forecast growth of the public safety sector according to ResearchAndMarkets. It is expected that Evolved 5G will accelerate growth of such applications.

FIDAL represents a convergence of key enabling technologies driving the growth of the PPDR market in the foreseeable future. It allows vendors in the market to rapidly deploy and extensively experiment on-demand with new solutions under various network conditions, thus improving their offerings.

3.2 High-level use case description

This section provides an overview and the motivation for each UC.

In particular:

- **Problem description:** what the UC is addressing?
- **Gap analysis:** which problem(s) the use case has the ambition to cover?
- **Impacted stakeholders:** all the actors involved and/or can benefit by the implementation of the use case?
- **What is to be provided as a new feature:** what is new in terms of service or new technology w.r.t. the state of the art and similar behaviour currently available?

3.2.1 Media vertical industries

1. UC1 Internet of senses/haptic sensing

- **Problem description:** Police and military training is currently very limited by the technology and the risks of practicing in a realistic scenario. The need for a large physical space, the need for everyone to be in the same place or the lack of a sense of touch in training are some of the problems encountered when training in these fields. From OWO, through our haptic technology, we intend to take police and military training to another level, recreating virtual training scenarios that are as close as possible to reality, using 5G technology to support us in the necessary requirements to solve this problem.
- **Gap analysis:** This UC aims to use 5G technology, which will enable the training of multiple users with a high quality of use, allowing the use of cloud-hosted training, guaranteeing the quality of using the virtual world and the real sensations in real time, reducing latency and other requirements that will be marked in the KPIs.
- **Impacted stakeholders:** Different police forces, both local and national. Military and intervention corps. Training and training companies.
- **What is to be provided as a new feature:** This UC aims to offer the following:
 - Users will have access to uninterrupted streaming of high quality and performance for multiple users located in the same area. Also, they will have access to the sensations Network Applications without any interruption.
 - Police and military forces, and training companies, will have the ability to receive multiple streams of high and ultra-high quality to provide added value and immersive experience for the training.

2. UC4- Advanced sports area media services

- **Problem description:** Media is one the areas where 5G is expected to have major impact to. UC4 aims to demonstrate 5G and beyond in this area by performing field trials in a stadium, by allowing the streaming of User Generated Content (UGC). This means that in an event where a lot of people are present allowing UGC to be streamed and having it professionally produced, the added value of more view perspectives can be presented and provided to the end viewers without using professional equipment but standard 5G enabled mobile phones. Furthermore, professional equipment can take advantage of advanced capabilities by offering Ultra High Definition (UHD – 8K) and 360° AR/VR media content.
- **Gap analysis:** This UC aims to explore and verify the beyond 5G capabilities of achieving multiple uplink streams of high-quality while at the same time respecting the requirements that will be set by Key Performance Indicators (KPIs) like throughput and latency. Furthermore, guaranteed performance functionality will also be explored to cover other aspects of media production.
- **Impacted stakeholders:** Media production companies, media producers, streaming companies, event managers, venue owners.
- **What is to be provided as a new feature:** This UC aims to offer the following:
 - Users will have access to uninterrupted streaming of high quality and performance for multiple users located in the same area.
 - Media companies will have the ability to receive multiple streams of high and ultra-high quality to provide added value and immersive experience for the covered event.
 - Professional coverage of an event will be assisted by guaranteed high performance services through the beyond 5G networks.

3. UC5- Virtual reality networked music performance

- **Problem description:** The network music performance (NMP) use case involves two scenarios: remote playing of music (1) and remote concert performance (2). The former involves musicians playing (teaching and rehearsal) together although from different locations, that aim to play together. The other scenario involves musicians (inclusion guest stars), some locally present and some remote, playing together live in a concert, with in presence and remote audience. This UC must also be seen as a proxy for handling of real-time predictable and specialised media capabilities embedded into or along with network capabilities is seen as an attractive opportunity of relevance to a wide range of use cases such as Emergency/Blue light services (Health, Fire, Defence, Police) as well as in a variety of industry applications. The problem for professional and amateur

musicians, they require to have easy to use, easy to setup, reliable, high bandwidth, and low latency communication platform (including devices and network) with a very simple interface that does not require the musician to be a network engineer. Video capturing setup and equipment also have to be simple, with a reduced cost, such as by using smartphones or entry level cameras (i.e., GoPro).

- **Gap analysis:** The main challenge for a technology to enable remote musicians to co-play is the audio and video latency between musicians, that must be as low as possible (below 30ms of round-trip delay). This target is necessary to meet, for the audience to perceive the music as a synchronic play. Being able to provide live performance to remote spectators, video is a highly important media type complementing the audio media type. Distributing low latency video over Internet requires high bandwidth reliable networks currently challenging to obtain as of today.
- **Impacted stakeholders:** The two use case scenarios involve stakeholders such as musicians, producers, concert hall/music festivals/recording studios. Moreover, it includes organisers and producers of NMP events and other actors involves such as telecom/ICT providers, e.g., Telenor and EKTACOM. With reference to NMP being a proxy for other use cases, emergency personnel and blue light service actors could also be relevant stakeholders to include.
- **What is to be provided as a new feature:** Beyond 5G will provide the necessary capacities for NMP use cases scenarios with network slicing, high bitrate, and low latency features. Lower price than fibre installations will be a key issue for making NMP accessible to non-renowned artists, and to small theatre and studios, or even artists playing from their home living place in the case of a pandemic lockdown. Beyond 5G will also enable NMP scenarios to and from non-permanent locations, for example for concerts that take place during music festivals, that can take place in lands and not in concert halls. The same features are also enablers for real time interaction between stakeholders (e.g., emergency, industry operator/expert) in rural areas/communities.

4. UC7- Smart village engagement services

- **Problem description:** This UC involves two scenarios: 1) co-created engagement in urban and 2) co-created engagement in rural communities. The problem in the first scenario is the limited opportunity for citizens and other community stakeholders for real time co-creation and involvement in the decisions process for development of urban areas in cities. The second scenario involves co-creation in rural areas. Here the problem is to coordinate the different public and non-profit emergency resources in case of accidents related to industry and/or forest/agriculture.
- **Gap analysis:** For the co-created engagement in urban areas scenario (1), there is a gap in real time virtual/digital access to co-development of urban plans, access to city assets/data on buildings, bridges, towers, dams etc. for large scale testing for application vendors and low latency wireless networks for real time handling. The latter is also the case for the second scenario (co-created engagement in rural areas scenario). Here the challenge is to quickly establish a service for distribution of real time situation awareness for involving personnel in emergency is areas with limited infrastructure and low coverage.
- **Impacted stakeholders:** In scenario 1 the major actors are citizens, city authorities and representatives from sectors in municipality, application providers and equipment vendors, technology/network provider etc. Scenario 2 also involves stakeholders from public stakeholders such as emergency/Blue light services (Health, Fire, Defence. Police) as well as stakeholders from the primary and service industry. Providers of telecom services are included in both scenarios.
- **What is to be provided as a new feature:** For scenario 1 we foresee use of VR/AR tools for real time joint interaction on digital platforms/digital twins and open public data for development and trials/pilots of proof-of-concepts. For scenario 2 we also foresee VR/AR tools to enhance supervision/operation for mission critical services (fire, police emergency teams etc) in rural areas. Here drones with 5G network antennas and video cameras distributing real time pictures and videos of the situation to emergence personnel involved.

3.2.2 PPDR vertical industries

1. UC2- Digital twin for first responders



- **Problem description:** In UC2, FIDAL will demonstrate the automatic deployment of hazard detection and monitoring algorithms for continuous updating of first responders about the future condition of the hazard evolution and short-term risk assessment, including i. Situation monitoring of the fire, ii. Monitoring of the ground assets, iii. Predicting fire propagation against environmental conditions and iv. Fire propagation disseminated to mobile users.
- **Gap analysis:** This UC aims to take advantage of the beyond 5G capabilities, such as the low latency, the high throughput, the high position accuracy and the video streaming capabilities, in order to achieve multiple uplink streams of high quality while monitoring the situation and disseminating information to the first responders on the field.
- **Impacted stakeholders:** Personnel from Civil Protection and Fire service agencies that are involved in the monitoring, management, and response of such situations.
- **What is to be provided as a new feature:** In PPDR digital twins are virtual representations of the real-life situation (including events, process, and environments) in real-time. First responders in wildfire situations face a large spectrum of challenges in disaster environments including environments with low visibility and hidden hazards:
 - Ability to stream high-resolution image frames from cameras without the need for microwave link and line of sight for AI-based forest fire and smoke detection.
 - Ability to disseminate fire propagation data to first responders in the field of forest in real time.
 - Real-time tracking of responders with the ability to know their precise position and their proximity to threats and hazards (between command and control and First Responders, between and inside operative units).
 - Integration of information for incorporating predictive information from multiple and non-traditional sources into incident command operations for obtaining position of assets and creating complete situational awareness

The use of digital twins capitalising on 5G evolution architectures and performance characteristics will address these challenges, by providing firefighters accurate and timely guidance and decision support for adapting the operations in a very dynamic environment.

2. UC3- City security event / incident

- **Problem description:** City area coverage with 5G evolution capabilities for the PPDR organisations involved, such as, but not limited to i. Slices (per organisation, per service / application), implemented as 3GPP slices or as private networks (MOCN or alternative mechanism), ii. High-quality real-time video stream sharing within groups of PPDR users with high density of concurrent users and iii. Ultra-Low Latency for Mission Critical PPDR operations.
- **Gap analysis:** Infrastructure area coverage with 5G evolution capabilities for the PPDR organisations involved, such as, but not limited to i. Slices (per organisation, per service / application), implemented as 3GPP slices or as private networks (MOCN or alternative mechanism), ii. High-quality real-time video stream sharing within groups of PPDR users with high density of concurrent users and iii. Ultra-Low Latency for Mission Critical PPDR operations (UAV).
- **Impacted stakeholders:** PPDR organisations, end-user verticals (law enforcement, medical, firefighting, etc.).
- **What is to be provided as a new feature:** Public Safety users have an increasing need for collection and exchange of information, including data, pictures, and video, along with voice, in real time and, above all, in a secure manner to carry out complex missions successfully. Effective, resilient, and secure collaboration and real time information sharing from various sources in various formats within groups of First Responders or other safety and security related organisations personnel and between safety and security authorities and organisations is a must when it comes to major events, incidents or natural disasters. As a matter of fact, recent advancements in Artificial Intelligence (AI), Internet of Things (IoT), Virtual, Augmented and Mixed Reality (VR, AR, MR) and powerful analytics can offer a number of desired capabilities to practitioners. This use case will demonstrate the benefit of 5G evolution network architecture and increased KPIs performance

capabilities for PPDR smart situational awareness and operational efficiency, and ultimately for people and PPDR users' safety and security.

3. UC6 XR-assisted services for public safety

- **Problem description:** First responders are usually not highly trained in surgical procedures. In many PPDR cases there are on-site incidents where there is a need for advanced operations. XR-assisted emergency surgical operations UC will provide the PPDR first-aid responders the ability to visualise, via an AR Head-Mounted Display (HMD), deformable medical-related objects and information on top of an injured person, such as bones, organs, and arteries. Furthermore, the first responder will be able to obtain step-by-step instructions regarding critical first aid and medical operations. Additionally, indoor medical experts, using VR HMDs, will collaborate with the first responders in the same XR scene, providing medical assistance and expertise in real-time, without having to move to the incident site. This use case ultimately aims to provide first aid responders on the PPDR scene with a powerful tool that will help save lives in peril. On the other hand, in public safety situations of high risk, such as terrorist attacks, the capability of rapid and effective decision-making constitutes number one factor of success. To that end, smart policing leveraged by disruptive technologies such as AI and AR, is of prominent importance for Law Enforcement Agents, towards enhancing their situation awareness on the field and thus achieving high levels of successful decisions. In the context of this UC, an AR framework for leveraging LEAs situation awareness will be deployed, incorporating the advantages offered by both AR and AI to realise technology-assisted policing in ways that have previously only been imagined in science fiction. Police officers will patrol and respond to incidents using wearable gear that will utilise AI in the form of Machine Learning routines to enable rapid scene analysis and interpretation to capture, outline and single-out interesting findings and threats requiring the attention of the smart glasses wearer. AR will then be used to superimpose such mission-critical information directly on top of the real world, catering to the officer's unique point of view, and ensuring a functional visualisation experience, meant to enhance the officer's capacity to respond to incidents.
- **Gap analysis:** This UC aims to explore and verify the beyond-5G capabilities of achieving multiple downlink and uplink streams of high-quality. Furthermore, Key Performance Indicators (KPIs) like throughput and latency are critical factors to preserve user immersion in the virtual scene.
- **Impacted stakeholders:** PPDR organisations, first aid responders, injured people, medical experts.
- **What is to be provided as a new feature:** This UC aims to offer the following:
 - First responders will have the ability to visualize deformable medical-related objects and information on top of an injured person and step by step instructions of critical first aid operations.
 - First aid responders will be in direct communication with indoor medical experts.
 - Medical experts will be able to visualize in VR the patient's avatar Medical and collaborate with the first-aid responders in the same multi-user 3D scene.
 - Law Enforcement Agents, prosecuting perpetrators on site, will be able to collectively enhance their situational awareness using advanced AI and AR technologies through which will be able to rapidly analyse and identify their targets.

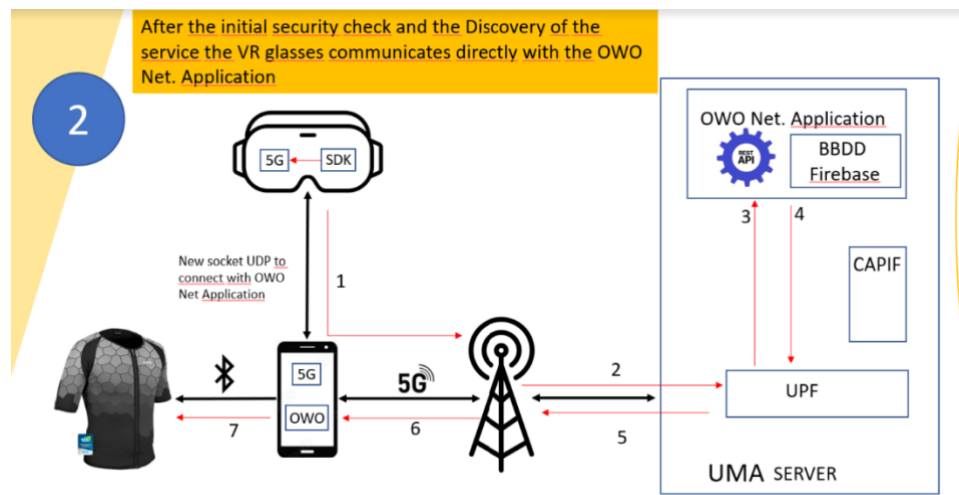


Figure 7: UC1 Workflow Diagram 2.

4.2 Stakeholders

4.2.1 Stakeholders' identification

Here are the identified stakeholders for this specific Use Case:

- Malaga local police;
- Other security forces;
- Partners involved in this Use Case: ADS UMA, TID.

4.2.2 Stakeholders' benefits

The identified benefits for the stakeholders in the context of UC1 are an improved quality of training through technology, enabling training at the same time in different locations. In addition, improve not only technologically, but psychologically, through the introduction of the sense of touch, analysing how the trainee reacts to physical interactions.

4.2.3 Stakeholders needs

- Access to 5G environment to ensure the good quality of the training and the correct functioning of the session.
- Training platform or virtual training environment with adaptation of OWO technology.
- OWO App in a smartphone to send the sensations received from the Net Application to the vest.
- VR headsets for each member practising to have access to the virtual training.
- OWO Vest to receive the physical sensations during the training.
- External physical elements for training immersion.

4.3 How can beyond 5G networks benefit the UC

5G technology will facilitate the speed, connection capacity and offloading of everything needed to enable multiple people to train at the same time in different locations.

4.4 Technology needs

4.4.1 5G services needs

- URLLC (Ultra-Reliable, Low-Latency Communications) - Critical Communications refers to latency sensitive, wireless applications and services, some of which are impossible to be supported by existing network deployments.

- Orchestration and Management to ensure the synchronization of the virtual training and the reception of the sensations.
- Location management functions to precisely know the current position of all members while training.

4.4.2 Network Application needs

- 5G environment to ensure the quality of the training due to the delays.
- Training platform or virtual training environment with adaptation of OWO technology.
- OWO App to send the sensations to the vest.

4.4.3 Equipment needs

The following equipment is necessary for the implementation of the Use Case:

- Smartphone devices where the OWO Application will be installed.
- VR headsets which to have access to the virtual training scenario.
- OWO Vest to feel real physical sensations while training.
- External physical elements for training immersion.
- 5G network elements to ensure the communications between headsets and with the API.

4.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC1:

Table 29: Target technological KPIs for UC1.

Key Performance Indicators (KPIs)	Value	Units
MSKPI-01: App/Server Accessibility	100	%
MSKPI-02: Content Load time/time to first picture	0.1	sec
MSKPI-03: Content Stall/Freeze	0	%
MSKPI-04: Content Download Throughput	20	Gbps
MSKPI-05: Content Upload Throughput	5	Gbps
MSKPI-06: Application service creation	<5	min
MSKPI-07: Network Applications deployment time	<5	min
Latency	<50	msec
Connectivity (users simultaneous connected)	>10	

4.6 KVIs

The following table maps the minimum set of KVIs to be evaluated within the context of UC1 in relation to FIDAL objective:

Table 30: KV's of initial potential relevance for UC1.

Key Value Theme	UC1 – Internet of Senses/Haptic Sensing
Democracy	
Trustworthy	Dependable, consistent, low error rates
Transparency	Auditability, understandability, and justifiability
Privacy	Privacy concerns of PPDR forces addressed
Economic Ecosystem (part of sustainable 6G)	
Economic Sustainability	Potential to increase market space

Business Value	Low cost and time to solve existing problems, increase training flexibility
Innovation	
Responsibility	Accountability mechanisms for system behaviour
Open collaboration	Collaborate with diverse end-users to develop responsibility requirements and risks, in particular
Flexibility	Aim to re-use existing infrastructure and be flexibly deployed
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Will seek to reduce environmental footprint and energy degradation due to activity
Waste Management	Will seek to reduce waste of physical resources without countering the savings with increased energy use.
Safety and Security	
Safety	improve societal safety and risk management to reduce injuries to PPDR
Security	Vulnerabilities identified and fixed and system secured
Data protection	Personal data protected from unauthorised use with accountability mechanisms in place
Societal Ecosystem (part of 6G for sustainability)	
Knowledge	Enhanced access to knowledge, training of PPDR and industry
Quality of Living / Wellbeing	Support improved wellbeing of PPDR

5 UC2 - Digital twin for first responders

Climate change has led to more frequent and severe wildfires in many parts of the world. Managing fires under these evolving climate conditions requires adaptive strategies and a comprehensive understanding of fire behaviour. 5G technology offers several advantages in the context of forest fire management. It enables high-speed and low-latency communication, allowing for real-time data transmission. With 5G, high-definition video streaming becomes feasible in remote areas. This allows for live video feeds from surveillance cameras, and other monitoring devices installed in forests. Emergency responders can remotely monitor the fire's progression, identify potential hazards, and make informed decisions in real time, improving situational awareness. Additionally, 5G networks provide reliable and high-bandwidth communication channels for emergency responders, enabling seamless communication among firefighters, incident commanders, and other stakeholders. They can exchange critical information, coordinate efforts, and respond effectively to evolving situations. The use case will demonstrate the capabilities of the 5G technology and the advantages it provides to the domain of forest fire detection and management.

5.1 Scenarios, contexts, and workflows

In the context of the UC2, the detection and management of a forest fire incident, using 5G technology will be demonstrated. A command centre will be deployed providing all the required situation monitoring and management operations. Additionally, several first responders will be deployed on the field, that will be equipped with handheld mobile devices. Both the command centre and the mobile devices will be connected to the 5G network, enabling the sharing of operational information in real time. Thus, information such as decisions taken, high-resolution maps, high-resolution video streams and images from the field will be shared. A number of cameras will be deployed (on the field), monitoring the area for smoke and fires. High-resolution streams will be created and forwarded through the 5G network to the advanced automatic fire detection module that will analyse the stream, identifying fire ignition points. Next, using this information, the propagation of the fire will be calculated. This information will be transmitted to the command centre and the first responders that will be on the field. Additionally, the real-time tracking of these responders and their proximity to threats and hazards will be provided to the command centres.

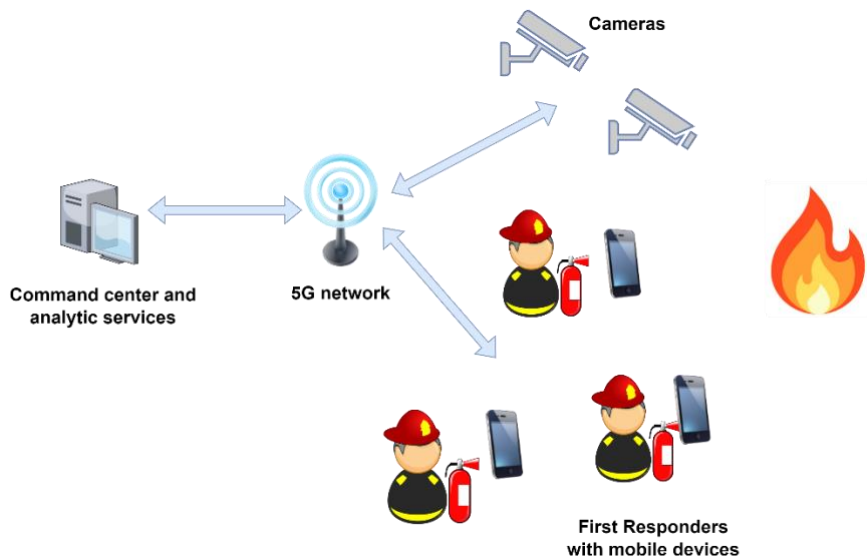


Figure 8: UC2 Workflow Diagram.

5.2 Stakeholders

5.2.1 Stakeholders' identification

Here are the identified stakeholders for this specific Use Case:

- Civil protection and fire service authorities;
- Partners involved in this Use Case: UoP, PNET, NOVA.

5.2.2 Stakeholders' benefits

The capabilities of the 5G network will improve the situation awareness of the first responders that are involved in a situation. These advantages contribute to early detection, rapid response, and effective firefighting strategies, ultimately helping to mitigate the impact of forest fires.

5.2.3 Stakeholders needs

- Transmission of multiple high-resolution video streams in real-time;
- Transmission of multimedia communication with low latency;
- Intelligent situation awareness, such as event detection and hazard propagation;
- Accurate localisation of first responders that will be deployed on the field.

5.3 How can beyond 5G networks benefit the UC

The UC will take advantage of the following 5G network capabilities:

1. Private network, in order to ensure secure communication among the responders.
2. High throughput, in order to ensure the streaming of multiple high-resolution video streams.
3. Low latency, in order to ensure the quick and accurate dissemination of the operational information to the responders.
4. Accurate localisation, in order to ensure the real-time tracking of the responders in high precision.

5.4 Technology needs

5.4.1 5G services needs

- URLLC (Ultra-Reliable, Low-Latency Communications);
- Orchestration and Management;
- Location management function.

5.4.2 Network Applications needs

- Video streaming management service that will handle the multiple streams that will be available.
- Automatic fire detection and propagation module, that will collect the video streams in order to analyse these and detect possible fire ignition points.
- An incident management system that will enable the monitoring and management of the situation. It will collect operational information from the several components that will be collected to the network and enable the management and communication with the first responders.
- Mobile devices that will be used by the first responders in order to exchange operational information.

5.4.3 Equipment needs

The following equipment is necessary for the implementation of the Use Case:

- 5G high-resolution cameras.
- 5G network elements.
- Smartphone and tablet devices.

5.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC2:

Table 31: Target technological KPIs for UC2.

Key Performance Indicators (KPIs)	Value	Units
-----------------------------------	-------	-------

PSKPI-01: Peak Throughput	5 UL/20 DL	Gbps/DL/UL
PSKPI-02: Application latency	<40	ms
PSKPI-03: Positioning accuracy	1	meter
PSKPI-04: User density connectivity	0.05 >10	Devices/m ² Nb users
PSKPI-05: Video resolution	72-144x30	x fps x no of simultaneous videos
PSKPI-06: Application service creation	<5	min
PSKPI-07: Network Applications deployment time	<5	min
UC2KPI-01: High throughput	>5	High-resolution concurrent video streams
UC2KPI-02: Latency reduction below	<40	ms
UC2KPI-03: Position	1	meter
UC2KPI-04: Simultaneous connection capacity	>10	users

5.6 KVs

The following table maps the minimum set of KVs to be evaluated within the context of UC2 in relation to FIDAL objective:

Table 32: KV's of initial potential relevance for UC2.

Key Value Theme	UC2 - Digital twin for first responders
Democracy	
Trustworthy	Dependable, consistent, low error rates
Inclusiveness / Equal Opportunity	Increased service availability and access
Transparency	Understandability, explainability, scrutiny
Economic Ecosystem (part of sustainable 6G)	
Business Value	Solve existing and emerging problems, reduce resources needed to engage
Innovation	
Responsibility	User control of system behaviour, clear chains of responsibility
Open collaboration	Improved awareness of stakeholder values, needs, and challenges
Flexibility	Dynamic optimal resource allocation and repurposing
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Reduced energy consumption, air pollution
Mitigation Strategies	Greater understanding of environmental challenges from tech
Compliance Quality Standards	Engage certification processes
Safety and Security	
Safety	Greater protection of vulnerable people, improved feeling safe, and increased operational efficiency for saving lives
Security	Decrease system vulnerabilities
Societal Ecosystem (part of 6G for sustainability)	
Healthier community	Improved satisfaction and access to services

6 UC3 – City security event / incident

Public Safety users have an increasing need for collection and exchange of information, including data, pictures, and video, along with voice, in real time and, above all, in a secure manner to carry out complex missions successfully. Effective, resilient, and secure collaboration and real time information sharing from various sources in various formats within groups of safety and security related organisations personnel and between safety and security authorities and organisations is a must. As a matter of fact, recent advancements in Artificial Intelligence (AI), Internet of Things (IoT), Virtual, Augmented and Mixed Reality (VR, AR, MR) and powerful analytics can offer several desired capabilities to practitioners. This use case will demonstrate the benefit of 5G evolution network architecture and increased KPIs performance capabilities for PPDR smart situational awareness and operational efficiency, and ultimately for people and PPDR users' safety and security.

6.1 Scenarios, contexts, and workflows

6.1.1 Scenario1: Critical infrastructure surveillance and inspection

The scenario is to increase the surveillance and inspection capacity on a critical infrastructure (Malaga city centre). At first, PPDR mobile users and dispatchers will be able to experiment with Mission Critical Services (MCS) applications enabling the following functionalities:

- Group and individual voice calls (Push to Talk/Full Duplex).
- Group and individual messaging.
- Group and individual multimedia messaging.
- Individual video calls.
- Emergency calls.
- Location and map services.

The use of UAV will be a significant advantage as it allows a quick and wide coverage zone.

The video streams (UAV and other cameras) are transmitted to the dispatcher in real time in low quality, in order to save energy and bandwidth, especially for the UAV. Regarding the situation, the video stream quality could be improved to higher resolution for better situation analysis.

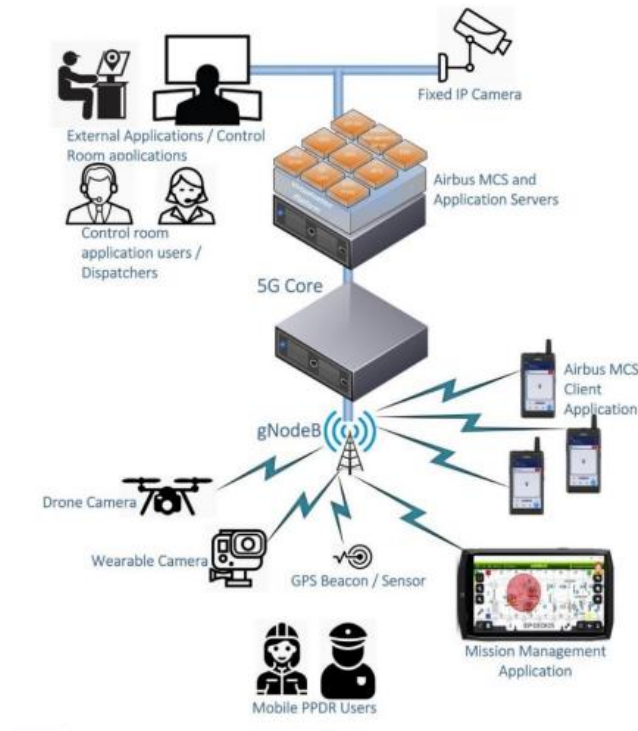


Figure 9: UC3 Workflow Diagram.

6.2 Stakeholders

6.2.1 Stakeholders' identification

Here are the identified stakeholders for this specific Use Case:

- Police forces (through Open Calls);
- Fire fighters brigade (through Open Calls);
- Partners involved in this Use Case: ADS, UMA, TID.

6.2.2 Stakeholders' benefits

Critical infrastructure surveillance involves various PPDR organizations (e.g., fire fighters, police, local organisations, private organisations), with field operation being coordinated both in local field commander positions and control centers, and by the remote headquarters. The goal is to validate the applicability, performance and benefits of the project for supporting Mission Critical multimedia communication in critical infrastructure scenarios, and its interaction with data-centric IoT technologies to improve event identification and characterisation, operation by PPDR organisations.

During critical infrastructure scenarios, decisions and operations should be strongly aided by technologies such as communication networks, multi-source data and IoT analysis and assisted decision-making platforms, including UAVs / drones which are used both for realizing data collection (e.g., visible & thermal image, geo-references) and mission support (e.g., equipment delivery, signal repeating).

6.2.3 Stakeholders needs

- End-2-End Secured Multimedia Communication.
- Secured transmission in real time adaptive video streams.
- Intelligent situation awareness, such as event detection (intrusion, fire, etc.).
- Accurate localization to guide UAV/PPDR teams.
- Secured remote control of the UAV.

6.3 How can beyond 5G networks benefit the UC

Infrastructure area coverage with 5G evolution capabilities for the PPDR organisations involved, such as, but not limited to i. Slices (per organisation, per service / application), implemented as 3GPP slices or as private networks (MOCN or alternative mechanism), ii. High-quality real-time video stream sharing within groups of PPDR users with high density of concurrent users and iii. Ultra-Low Latency for Mission Critical PPDR operations (UAV).

6.4 Technology needs

6.4.1 5G services needs

- URLLC (Ultra-Reliable, Low-Latency Communications) - Critical Communications refers to latency sensitive, wireless applications and services, some of which are impossible to be supported by existing network deployments. These services are referred also as “mission-critical” communications or critical Machine-Type Communications (cMTC) (by 3GPP), and include public safety lifeline and situational awareness, industrial automation, drone control, new medical applications, autonomous vehicles, etc.
- E2E Slice in order to enable different priority levels for different users and different communication types.
- Orchestration and Management.
- Location management function.

6.4.2 Network Application needs

- Airbus MCS Server: this VNF contains all the necessary modules for the control and management of voice, video, and data communications. This includes an MCS Controlling Server, an MCS Participating Server, an Identity Management Server (IdMS), a Key Management Server (KMS), a Group Management Server (GMS), a Configuration Management Server (CMS), a SIP Core, an HTTP Proxy and an MCS Configuration Server.
- Airbus MCS API Gateway: this VNF implements the gateway which manages incoming API requests from external applications and routes them to the right MCS Server module. It also sends the API responses back to the application.
- Airbus Map Server: this VNF hosts the map and provides the map elements (tiles) to the MCS clients.
- Airbus Mission Management Server: this VNF enables a mobile client to download and install a mobile application for tactical situation awareness which provides geographical information, PPDR resource allocation and instant messaging.
- DNS Server: this VNF provides a name server based on the DNS.
- NTP Server: this VNF provides a Network Time Protocol (NTP)-based server.

6.4.3 Equipment needs

- Smartphone and tablet devices.
- 5G network elements.
- External 5G video sources such as Wearable Camera, Drone Cameras, and Fixed Cameras. Could use cameras with 5GNR modems.

6.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC3:

Table 33: Target technological KPIs for UC3.

Key Performance Indicators (KPIs)	Value	Units
PSKPI-01: Peak Throughput	5 UL/20 DL	Gbps/DL/UL
PSKPI-02: Application latency	<10	ms

Latency (air interface)	<2	
PSKPI-03: Positioning accuracy	1	meter
PSKPI-04: User density	0.05	devices/m ²
PSKPI-05: Video resolution	72-144x30	x fps x no of simultaneous videos
PSKPI-06: Application service creation	<5	min
PSKPI-07: Network Applications deployment time	<5	min

6.6 KVis

The following table maps the minimum set of KVis to be evaluated within the context of UC3 in relation to FIDAL objective:

Table 34: KV's of initial potential relevance for UC3.

Key Value Theme	UC3 - City security event / incident
Democracy	
Trustworthy	reliability, consistency, dependability
Inclusiveness / Equal Opportunity	Increased service availability and access
Fairness	Lack of bias
Personal freedom	Human-in-the-loop, ability to make decisions
Transparency	Understandable in how it fits within current practices
Privacy	Privacy preserving
Economic Ecosystem (part of sustainable 6G)	
Economic Sustainability	Reducing costs by using existing systems rather than building new one
Business Value	Perception of problems solved, business plans
Innovation	
Responsibility	Accountability for system behaviour, enables alternative approaches
Open collaboration	Placing users at the centre of the design process
Flexibility	Optimal resource allocation, re-use of existing systems, ability of AI systems to adapt
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Reduction of energy consumption, decreased energy degradation
Waste Management	Re-used and re-purposed existing equipment
Safety and Security	
Safety	Greater protection of vulnerable people, improved feeling safe, and increased operational efficiency for saving lives
Security	Quality of services, End-to-end security of the mission-critical
Data protection	GDPR compliance
Societal Ecosystem (part of 6G for sustainability)	
Societal sustainability	representation in use cases
Healthier community	Improved relationships with organisations, improved health
Knowledge	Enhanced technical and research skills

7 UC4 – Advanced sports area media services

The emergence of 5G technology has opened new possibilities for innovative and engaging experiences in large sports events. With the increasing demand for real-time updates and immersive content, a new rich media content service application is developed and evaluated under FIDAL platform. The service targets to enhance the end-user in-stadium experience by allowing fans to access a wide range of multimedia content while also serving as the content provider in some cases. The content allows high-quality video feeds from different angles but can be extended to include features like UHD and 360° video as well as the use of augmented reality experiences, all in real-time in terms of end user perception. The application poses important challenges in terms of bandwidth management and scalability of resources as the number of end users increases. Video feed processing for quality and content homogeneity purposes, and especially low end-user perceived latency are also key characteristics that should be met especially for large scale service deployments.

7.1 Scenarios, contexts, and workflows

7.1.1 Scenario 4.1: Enriched high quality video content collection and distribution

This scenario considers first the upload of sport event media contents (e.g., UHD 8k and 360° VR) from several professionals or semi-professionals through a pusher application at the end-user device. It is noted that this content is additional to the live streaming video feed of the provider that is typically sent to the broadcaster premises through micro-wave links. The content is uploaded through advanced 5G connection with high availability and upload throughput, utilising techniques such as beamforming to achieve dedicated end-user high-capacity links and extreme upload speed capabilities. A stream selector and dispatching application (with both service- and network-level application components) is deployed at the edge or the core and across the continuum, according to the targeted KPIs under different load conditions. The application includes the following components:

- a video gateway for receiving multiple video streams from the video stream pusher application.
- a video mosaic builder for assembling all the collected material, with a video dispatcher at the input to feed the streams from the gateway.
- a transcoder for format adaptation and for enabling video preview.
- additional components for enhanced video stream processing to meet video transmission, format and quality standards.
- a stream selector and video player register for managing the end-users, the content to be uploaded, the supported formats and more.

At the receiving end-user site, a video player application is installed and connects to the stream selector and dispatching network application. Through this the end user can select which video feed to request and display.

7.1.2 Scenario 4.2: Event media content extensions including end-user generated video material

This scenario is an extension to the first one and includes the case of end-user generated video contents to be pushed through the video content management service (i.e., the stream selector and dispatching application). Registered end-users have the capability to push video streams with standard quality through the video stream pusher application on their end-devices. The challenge is to identify the system scalability in terms of registered end-users, while at the same time guarantee the quality of the video streams pushed through the first scenario. The workflow using the stream selector and dispatching application is the same as before but in this case the type of end users pushing their content is separated and guarantees are provided according to their type (i.e., high priority for professional end-users, best effort for registered end-users). The video player and content selection application are also adapted to host and provide the additional content. This is followed by related changes required in the video mosaic builder application component as well as the stream selector and video player register component. The scenario can be further extended to include inappropriate content detection components in the video processing stage.

The following figure provides the high-level representation for both scenarios, including all the considered deployment and end user options.

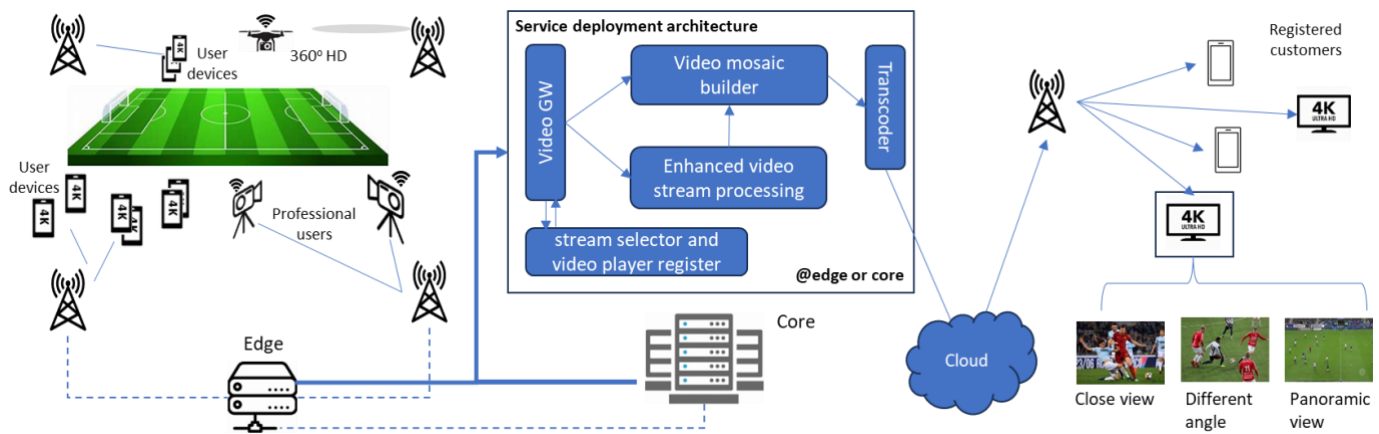


Figure 10: UC4 Workflow diagram

7.2 Stakeholders

7.2.1 Stakeholders' identification

Here are the identified stakeholders for this specific Use Case:

- **Media service providers:** The owners of rich media content that is provided through services to their customers.
- **Infrastructure owners:** The owners of the infrastructure that will guaranty the service deployment and delivery to the service provider(s). From market perspective this can split further to large infrastructure owners and owners of licensed 5G bands and supporting private infrastructure owners as for example stadium infrastructure owners with 5G connectivity capabilities (e.g., O-RAN based).
- **Application developers:** The providers of the application components required to offer a functional service or even developers of additional components with enriched capabilities typically in the broader field of media content management and video processing.

7.2.2 Stakeholders' benefits

Media service providers: This stakeholder group can be significantly benefited through the offering of advanced services to their customers, having a direct added market value. The market potential can vary according to the selected model, which may include increased revenues through services offered at an additional cost or an increase in the number of registered customers through the offered advance capabilities.

Infrastructure owners: The large infrastructure owners benefit from the increased usage of their infrastructure due to the offered services capabilities and the related revenue according to the agreement with the service provider. In the case of a private infrastructure owner, the key benefit is in the supported service capabilities which increases the attractiveness of the specific place for accommodating sport related or other events.

Application developers: The specific use case promotes the active involvement of 3rd party developers (individuals of SME in software development solutions) in the creation of advance specialised services and solutions, related with the fields of content management and video processing. The supported network application concept allows developers to provide targeted software component solutions that can be included as add-on to the service or as added value extensions, (rather than complete end-to-end services, typically requiring large development and testing teams).

7.2.3 Stakeholders needs

Here is a list of the needs from the various stakeholders (media owners, infrastructure owners, application developers) in the two scenarios included in this use case:

- Directional beam to meet ad hoc increased bandwidth needs.
- Low user perceived latency to enable synchronization of the generated content with the broadcasted stream.
- Dedicated slice setup to assist beyond UHD professional production, independently of the end-user generated content.

- Increased density to assist uninterrupted HD end-user generated content.
- Edge node pre-processing capabilities to assist the pushing of generated content by increased number of end-users.
- Authentication of registered end-users.
- (Optionally) Capabilities to examine the pushed media for inappropriate content or language.
- Seamless cross-domain operation for the interconnection of private 5G access domain to core infrastructure through the platform SBI.
- A clear and structured environment for the onboarding of application components and the creation of network application services.
- Support of containerized service deployments to assist updates and extensions.
- Application development process to be agnostic of the targeted infrastructure.
- Support of smart allocation of resources according to user profile and infrastructure needs.
- Support of dynamic upscale of resources to meet running application requirements (ideally defined by end-users through a policy mechanism linked to specific monitoring metrics).

7.3 How can beyond 5G networks benefit the UC

It is expected that 5G evolution will support the very high-density UHD and beyond uplink transmissions from the same location, avoiding congestion and supporting Network Applications workflows for such contents, all of which are not supported by existing 5G networks. When many people are at an event, e.g., in stadiums, then their UGC may provide additional “colour” content from various angles and perspectives. Using it in professional video production poses further challenges, such as ensuring quality, reliability, and authenticity. In addition, professional content encoding, transmission, and synchronization with external 4k and beyond video cameras must be ensured. This scenario will also explore the future of media consumption, which involves UHD 8k and 360° VR media content streamed over 5G evolution, and offering collaborative, interactive experiences. TV sets capable of 8k are already commercially available, while 8k-5G TVs have been announced and expected to be commercialized soon as the bandwidth and reliability required by 8k streams cannot be supported even by most wired broadband solutions today.

7.4 Technology needs

7.4.1 5G services needs

- uRLLC (Ultra-Reliable, Low-Latency Communications) service with additional high bandwidth connectivity capabilities for dedicated end users.
- eMBB (enhanced Mobile Broad-Band) service to scalable number of authorised end users.
- Two types of E2E slices, one per service type, for the same Network Applications and with enhanced guarantees for the uRLLC type, implementing different priority levels.
- Inclusion of end-user authentication services and optionally content verification service extensions.
- uRLLC services to professionals to be deployed at the edge node level.
- Smart allocation of eMBB service resources to support scale of end-users at expense of latency.
- Support of directional beam forming capabilities for specific end-users and increased density for large number of common registered end users, with priorities for the former case.

7.4.2 Network Application needs

- Video Gateway: Responsible for receiving video streams directly from the smart phone Video stream pusher App and dispatching them to video mosaic builder and transcoder.
- Video Mosaic Builder: as well as dispatching selected streams to targeted video players.
- Video transcoders: Responsible for enabling generation of video previews and potentially providing video correction capabilities.
- Video dispatching server: Responsible for dispatching selected streams to targeted video players (end user smart phone player applications).
- StreamSelector Register: Responsible to manage connections between video sources and destinations.

7.4.3 Equipment needs

- Smartphone and tablet devices.
- (Optionally) UHD cameras with 5G connectivity.
- Edge servers ideally with GPU processing capabilities.

- Antennas with beam forming capabilities.
- External 5G video sources such as Wearable Camera, Drone Cameras and Fixed Cameras. Could use cameras with 5G NR modems.

7.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC4:

Table 35: Target technological KPIs for UC4.

Key Performance Indicators (KPIs)	Value	Units
MSKPI-01: App/Server Accessibility	100	%
MSKPI-02: Content Load time/time to first picture	0.1	sec
MSKPI-03: Content Stall/Freeze	0	%
MSKPI-04: Content Download Throughput	NA	Gbps
MSKPI-05: Content Upload Throughput	5	Gbps
MSKPI-06: Application service creation	<5	min
MSKPI-07: Network Applications deployment time	<5	min

7.6 KVs

The following table maps the minimum set of KVs to be evaluated within the context of UC4 in relation to FIDAL objective:

Table 36: KV's of initial potential relevance for UC4.

Key Value Theme	UC4 - Advanced sports area media services
Democracy	
Trustworthy	Quality characteristics and the availability of service
Inclusiveness / Equal Opportunity	Spread benefit of sports across spaces, available to all
Fairness	lack of bias, available to all
Personal freedom	Maintaining dignity
Transparency	auditability
Privacy	Privacy of what users watch and consume
Economic Ecosystem (part of sustainable 6G)	
Economic Sustainability	Create new services, increase quality of services, lower costs; Maintaining compatibility to standards and open architectures will increase participation from the business sector
Business Value	Ability to produce additional functionality and content; New value chain in network operation and onboarding content
Tackling economic inequality	Lower costs and increase access/relevance of services across socio-economic demographics
Innovation	
Responsibility	Accountable risk management oversight
Flexibility	Ability of AI models to adapt to different conditions
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Lower energy consumption, optimise use of resources
Safety and Security	
Safety	Increased sense of safety of those at events
Data protection	GDPR compliant

Societal Ecosystem (part of 6G for sustainability)	
Societal sustainability	New services and devices for all people
Cultural connection	Improved access to cultural products and events
Knowledge	Collaboration of various technical and engineering groups will increase knowledge and cross-sector skill development

8 UC5 – Virtual reality networked music performance

8.1 Scenarios, contexts, and workflows

Networked Music Performance (NMP) is the name given to music played live, between remote musicians, through audio over IP technology, with or without the use of accompanying video. It enables musicians to perform together from different geographic locations. This requires capturing and transmitting audio streams through the Internet, which may introduce packet delays, packet losses and processing, capturing, and rendering delays that can have an impact on the feasibility of the performance. Figure 11 hereafter depicts a Networked Music Performance³².



Figure 11: Example of a Networked Music Performance .

The main challenge of such a technology is the audio latency between musicians, that has to be as low as possible (below 30ms of round-trip delay) with the aim of not providing annoyance that could impeach musicians to play together. In order to minimise this latency, audio can be distributed across the different musicians' locations, by using modern Audio over IP (AoIP) technologies such as Dante or AES67. These transport protocols use uncompressed audio, and therefore require high bitrate (around 2.8Mb/s for 24bit/96kHz PCM audio 2 channels (stereo), and much more when more channels are distributed). These transport protocols enable the distribution of a high number of audio channels (i.e., 64 channels per connection for AES67).

NMP covers a range of applications from remote auditions, remote music teaching, remote rehearsals and concerts that can take place on a fixed (e.g., concert hall) or in an ad-hoc location (like open air music festivals). The NMP use case is also a proxy for other use cases that requires or can benefit from specialized media capabilities and enablers in verticals such as Emergency/Blue light services (Health, Fire, Defence, Police) as well as in a variety of industry applications, just to mention a few. The NMP use case must be seen in this context where the offering and handling of real-time predictable and specialised media capabilities embedded into or along with network capabilities is seen as an attractive opportunity of relevance to a wide range of use cases. Extended UC definition or complementary UC definitions will be considered as time allows and as partnership collaboration matures.

³² For more information, see: <https://mdessen.medium.com/networked-music-performance-an-introduction-for-musicians-and-educators-d31d33716bd2>

In addition, for being able to provide live performance to remote spectators, but also for easing interactions between remote musicians, video is a highly important media type complementing the audio media type. But distributing low latency video over Internet requires high bandwidth reliable networks. Despite the work done by SMPTE Standard Organisation, with SMPTE ST 2110 standard, and its ST 2110-22 compressed video format (that can use the recent JPEG-XS codec), a minimum 3Gb/s bandwidth will be required for enough quality on Ultra HD video. In addition, in order to have a reliable connection and guaranteed bitrate, today it is necessary to rent a dedicated fibre connection, that is far beyond the price of consumer fibre connection prices.

In order to comply with lower bitrate capacities higher compression rates and other codecs can be used, but they provide higher latency than JPEG-XS. Use Case 5 will implement such codecs, with particular configurations in order to minimise this latency, while enabling audio to stay with low latency, and will add resynchronization features for delivery to the audience.

An overview of all of the data interactions is illustrated in Figure 12:

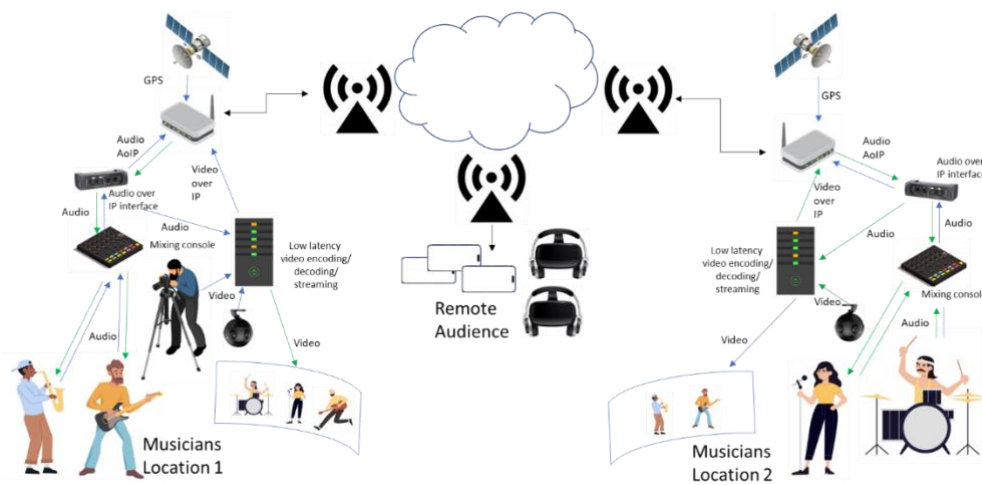


Figure 12: Data interaction overview for UC5.

Two different scenarios are considered in FIDAL, both requesting the common use of video and audio:

- remote teaching of music, with individual or several students playing together;
- ensemble activity for distant or socially isolated musicians (e.g., rehearsal).

8.1.1 Scenario 5.1: Remote playing of music

This scenario involves musicians present on different locations, that aim to play together. Related application includes (not limited to).

- Remote teaching of music, with individual or several students playing together
- Ensemble activity for distant or socially isolated musicians (e.g rehearsal)

8.1.2 Scenario 5.2: Remote

This scenario involves musicians (some locally present and some remote) playing together live in a concert, with in presence and remote audience.

Related applications include (not limited to):

- Virtual concert, rendered simultaneously in different places, in addition to the potential physical location.
- Guest stars remote participation to concerts and festivals without being physically present (Hybrid concert).

8.2 Stakeholders

8.2.1 Stakeholders' identification

Here are the identified stakeholders for this specific Use Case:

- Music students;
- Musicians, Producers (through Open Call);
- Concert Hall/Music Festivals/Recording studios (through Open Call);
- Networked Music Performance Organizer/Producer (through Open Call);
- Partners involved in this Use Case: TNOR, EKT.

With reference to NMP being a proxy for other use cases, emergency personnel and blue light service actors could also be relevant stakeholders to include.

8.2.2 Stakeholders benefits

Networked Music Performance technology:

- Provides improved means for remote teaching of music, with individual or several students playing together.
- Provides access to ensemble activity for distant or socially isolated musicians, whatever they are professionals or amateurs.
- Allows that guests can start remote participation to concerts and festivals without being physically present (reduction of participation cost for organizers, and less transportation pollution).
- Allows virtual, physical or hybrid concert, rendered simultaneously in different places.

8.2.3 Stakeholders needs

Whatever users are professionals or amateurs, they require to have easy to use, easy to setup, reliable, high bandwidth, and low latency communication platform (including devices and network). They would like to have financially accessible communication links, with the performance that can provide a dedicated fibre connection.

Easy to use and setup means a very simple interface that does not require the musician to be a network engineer. NMP equipment and/or software has to interface with existing audio equipment, used by musicians/sound engineers in (home)studios, in analogue or digital, including Audio over IP equipment like Dante. Video capturing setup and equipment has to be simple, with a reduced cost, such as by using smartphones or entry level cameras (i.e., GoPro like). Video images have to remain synchronised with audio when rendered at a remote location. All musician locations can see video from the others. Audio shall have the minimum latency, allowing musicians to play together from it, with a maximum of 30 to 50ms of delay depending upon the type of music). Video can be delayed from audio (in late) with a maximum delay of 120ms (lip-sync delay perception threshold).

8.3 How can beyond 5G networks benefit the UC

Until now NMP on stage performance was established with the support of dedicated point to point optic fibre connections. This requires costly infrastructure and fixed locations where to operate. Anyway, this can provide a reliable high bitrate and ultra-low latency remote connection between musicians, but with the drawback of a costly installation, that will restrict usage to top level artists.

Beyond 5G will enable NMP to be established without the requirement of having a costly reliable WAN connection such as dedicated or dark fibre. High bitrate, slicing and low latency features are key features for providing the necessary capacities for NMP. Lower price than fibre installations will be a key issue for making NMP accessible to non-renowned artists, and to small theatre and studios, or even artists playing from their home living place in the case of a pandemic lockdown. Beyond 5G will also enable NMP to and from non-permanent locations, for example for concerts that take place during music festivals, that can take place in lands and not in concert halls.



8.4 Technology needs

The above introduces technology needs for the networked music performance use case. QoS and QoE for the various NMP users should be tested, and relevant tools will help the efficiency of running test-cases and handling relevant data for the analysis of the UC.

In order to enable and support the above, complementary key technology needs are divided into 5G service needs, network application needs and finally equipment needs.

8.4.1 5G services needs

- eMBB (enhanced Mobile Broad-Band) service to CPE and other relevant devices.
- Secure access to the customer logical network (LNaaS).
- Setup and configuration of relevant and specialized QoS / QCI flows.
- Open APIs for request and configuration of “Specialized Connectivity Service” on-demand (optional).
- Management tool for efficient provisioning, management and administration of subscriptions, on-demand services and their SLAs for supporting multiple customers and users (Optional).

8.4.2 Network Application needs

As a baseline, use of the network applications as for UC4. However, the use of the relevant Network applications will be adapted for UC5.

8.4.3 Equipment needs

- Smartphone, CPE, and tablet devices.
- (Optionally) UHD cameras with 5G connectivity.
- Edge and central cloud server resources.

8.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC5. While these KPIs can be considered as target KPIs under excellent conditions we will also investigate elasticity of the KPIs in the context of different applications and their use case scenarios, exploring also when KPIs can be considered as “passed”, “partially passed” and “not passed”.

Table 37: Target technological KPIs for UC5.

Key Performance Indicators (KPIs)	Value	Units
MSKPI-01: App/Server Accessibility	100	%
MSKPI-02: Content Load time/time to first picture	0.1	sec
MSKPI-03: Content Stall/Freeze	0	%
MSKPI-04: Content Download Throughput	20	Gbps
MSKPI-05: Content Upload Throughput	5	Gbps
MSKPI-06: Application service creation	<5	min
MSKPI-07: Network Applications deployment time	<5	min
Network Latency	<30	ms

8.6 KVis

The following table maps the minimum set of KVis to be evaluated within the context of UC5 in relation to FIDAL objective:

Table 38: KV's of initial potential relevance for UC5.

Key Value Theme	UC5 - Virtual reality networked music performance
Democracy	
Trustworthy	Dependable, consistent, building confidence
Inclusiveness / Equal Opportunity	Service access and availability, local skill creation
Fairness	Fair distribution and access to music experiences
Personal freedom	Ability to choose when to join in to such activities
Transparency	Auditability, understandability
Privacy	support individual expression and right to assembly
Economic Ecosystem (part of sustainable 6G)	
Economic Sustainability	Improved opportunities for local communities
Business Value	New economic possibilities can emerge for both artists and technology companies
Tackling economic inequality	Market entry for smaller musicians and tech developers
Innovation	
Responsibility	All parties able to assess responsible use of the system
Open collaboration	Work with stakeholders to understand how connectivity can improve music experiences
Flexibility	Work in different environments and scales
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Decrease energy and resource use through digital connections, if new energy use is proportionate
Waste Management	Decrease waste through improved potential for virtual connection
Mitigation Strategies	Improved environmental monitoring of tools in ways that support stakeholders in developing mitigation strategies
Compliance Quality Standards	Working with compliance quality standards can support stakeholders in their own environmental assessments
Safety and Security	
Safety	Risk management, easy to use tools
Security	Decreased vulnerabilities; delegation of responsibilities
Data protection	Personal data protected with user control.
Societal Ecosystem (part of 6G for sustainability)	
Societal sustainability	Increased opportunity for musicians of all type to participate, collaborate, create, and have audiences; diverse representation in use cases
Cultural connection	Improved access to music, community culture, products
Knowledge	Improved knowledge of musical experiences as well as stakeholder knowledge of creative digital possibilities
Quality of Living / Wellbeing	Improve mental and social contentment

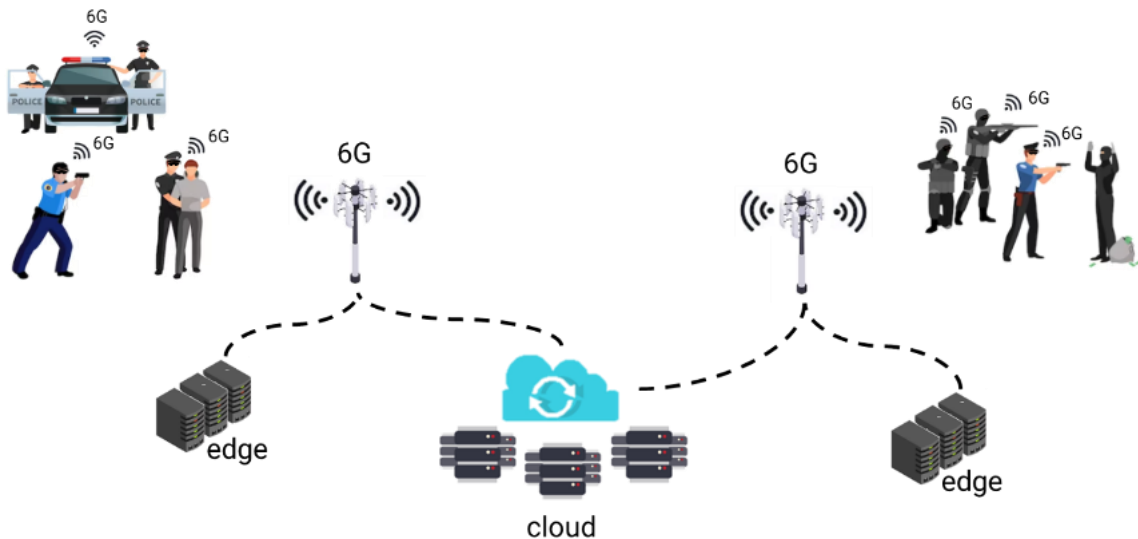


Figure 14: UC6 Workflow Diagram 2.

In this regard, the real-time performance of the incorporated algorithms, aside its obvious benefit for rapid decision making, also limit data recording and storage requirements for offline processing, thus alleviating ethical concerns related to storage and handling of massive data volumes. Furthermore, processing data on the edge will not only ease up communication requirements and decrease latency, but will enable in situ data processing thus avoiding privacy threats from cyber-security attacks (e.g., eavesdropping) during data transmission and cloud processing. To that end beyond 6G networks will provide the necessary capacity for accommodating large number of the provided AR technologies for LEAs at the same place, safeguarding the necessary low latency and high bandwidth demands which need to be ensured for the real-time process of the video-feeds from the LEAs' Head Up Displays.

9.1 Scenarios, contexts and workflows

In the context of an earthquake disaster, many injured people on the disaster site urgently need instant medical care. A number of first-aid responders are responsible of providing medical services to the injured. Some of the incidents require advanced medical expertise and the first-aid responders will utilize the untethered AR HMD application to get assistance. The main workflows are:

- a. A first-aid responder needs to view the deformable model of muscles and tendons for the right shoulder.
- b. A first-aid responder needs to view step-by-step instructions for a specific operation on the patient.
- c. A medical expert needs to collaborate with the first-aid responder to provide assistance on a specific surgical operation.

In the context of public safety scenarios, a big number of law enforcement tacticians and paramedics will be engaged in order to cater for the neutralization of a terrorist attack and provide triage services to the victims. The involved agents and practitioners will wield AR glasses incorporating the wearable AR framework for enhancing LEAs' situational awareness. The main workflows for the realization of this use case are:

- a. LEAs need to inspect the area and identify the number of perpetrators that exist in the area.
- b. Try to collectively neutralize the perpetrators, disarming them from carried weapons, while they inspect the area for any suspicious/dangerous objects (e.g., explosives).
- c. After the perpetrators have been prosecuted first aid practitioners wearing the same AR glasses will scout the area to identify civilians that need medical help as per the triage protocols.

9.2 Stakeholders

9.2.1 Stakeholders' identification

Here are the identified stakeholders for this specific Use Case:

- University of Patras first-aid responders;
- University of Patras medical experts;
- Citizens;
- Partners involved in this Use Case: ORAMA, FORTH, UoP, PNET, NOVA;
- Law Enforcement Agents.

9.2.2 Stakeholders' benefits

Here is a list of the identified stakeholders benefits for this specific Use Case:

- University of Patras first-aid responders will be able to advance their knowledge while providing high quality advanced medical services, utilizing the “On-site XR-assisted emergency surgical operations” use case application. The responder’s mobility will be enhanced since the AR HMD will be wirelessly connected to the 5G network and its battery life will be maximized since the heavy rendering and physics processes will be offloaded to edge resources.
- University of Patras medical experts will be able to provide real-time assistance to the first-aid responders without having to travel to the disaster site.
- Citizens will get high quality medical services from first-aid responders, assisted by medical experts.
- ORAMA use case application Quality of Experience (QoE) will be optimized to take advantage of the minimal latency and maximum bandwidth provided by beyond 5G networks.
- Law Enforcement Agents will benefit by using a system that leverages their situational awareness in the field of difficult operations for public safety.
- FORTH will expand their wearable AR framework by implementing the necessary Network App for the real-time video streaming and the AR annotation feedback loop.

9.2.3 Stakeholders needs

- Preserved AR/VR immersion at all times.
- Increased HMD battery life.
- Real-time synchronization of user actions with the projected images.
- Real-time collaboration of AR with VR users.
- High-density UHD and beyond uplink/downlink transmissions from the same geolocation.
- Real-time annotation feedback for the digital augmentation of the operation scene.

9.3 How can beyond 5G networks benefit the UC

Beyond 5G networks will play a central role in accelerating compute and connectivity transfers from edge resources to both wearable AR and VR devices. The mobility of first-aid responders on the disaster site is an important factor that should be supported by the PPDR system technology. This requires the use of AR HMDs that wirelessly connect to the broadband network. Immersion in VR/AR systems must be always maintained, making the ultra-low end-to-end latency a critical factor. Previous solutions (5G-EPICENTRE Network application) experienced controversial QoE, suffering from user event synchronization issues due to increased end-to-end latency and limited bandwidth. Beyond 5G networking is expected to support decreased latency and increased bandwidth to ensure transmission and synchronization of AR and VR HMDs for optimal QoE. Both uplink and downlink network throughput are equally important as the medical scenario will offer collaborative and interactive experiences between AR first-aid responders and VR medical experts. 5G evolution is expected to ensure such bi-directional media consumption. In disaster sites, many medical incidents need relief in parallel, meaning that a great number of a first-aid responders will use the AR PPDR system concurrently. This situation requires a high-density UHD and beyond uplink/downlink transmissions from the same geolocation, which may not be supported by 5G networks. Beyond 5G networking is expected to support such features that will avoid congestion and support the Network application workflow. The current wearable

Augmented Reality (AR) framework used by law enforcement agencies (LEAs) operates on a micro-device with limited AI inference capabilities that each LEA carries. In this FIDAL use case, it is expected that the testbeds provided will act as key enablers for achieving efficient and resilient offloading of the framework's intensive computations to edge or cloud infrastructure. This will result in improved performance and accuracy of the AI processes. The intelligent Zero-Touch orchestration and secure AI-as-a-service of the FIDAL system will facilitate the secure real-time migration of intensive and demanding processes along the edge-cloud continuum. Additionally, the improved network capabilities of the provisioned near-to-6G testbeds will enhance the situational awareness of the LEAs, enabling a large number of agents wearing AR glasses to collaboratively address and prosecute the perpetrators. To achieve this, during the execution of the use case, the framework's processing pipeline will be offloaded to powerful edge/cloud devices. The AR glasses of the LEAs will be connected to the provisioned network testbeds, allowing for real-time video stream analysis and annotation feedback with improved accuracy and timeliness by the AI modules running at the edge or cloud. Consequently, the use case will offer a collaborative and interactive AR experience among a large number of collocated LEAs, including both uplink and downlink capabilities.

9.4 Technology needs

9.4.1 5G services needs

- **Radio Access:** a service that will allow the connection of the HMDs with the beyond 5G network.
- **FIDAL Communication:** a service that will allow the communication of the HMDs with the FIDAL portal and the network application on edge.
- **Load Balancing Service:** a service used to allocate resources to multiple edge instances of the ORAMA's or FORTH's AR/VR application to optimize performance.
- **Orchestrator Service:** a service that automates the configuration, coordination, and management of the various microservices and network application edge-instances.
- **Linked Network Service:** a service that will allow the discovery of users and sessions that are already logged in and running respectively.

9.4.2 Network Application needs

- **ORAMA's Remote rendering/streaming network application:** a service used to render encode and stream AR/VR content from the edge instance to the HMD.
- **Relay server (Photon):** a service used in multi-user sessions to relay user actions/events/transformations to all session participants.
- **FORTH's AR visualisation application running on AR glasses which are connected to FIDAL's testbeds.** FORTH's wearable AR framework for enhancing LEA's situational awareness running on the FIDAL's edge/cloud infrastructure.

9.4.3 Equipment needs

- 5G WiFi routers;
- AR/VR HMDs;
- Edge devices with high-end GPUs;
- Edge devices with ML processing capabilities;
- Cloud VMs with CUDA support.

9.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC6:

Table 39: Target technological KPIs for UC6.

Key Performance Indicators (KPIs)	Value	Units
PSKPI-01: Peak Throughput	5 UL/20 DL	Gbps UL/Gbps DL
Average Throughput	160 UL/800 DL	Gbps UL/Gbps DL
Data rate HMD/edge	0.7	Gbps
PSKPI-02: Application latency UC6.1	<70	ms
Application latency UC6.2	<120	ms
E2E Latency	<=7	ms

PSKPI-03: Positioning accuracy	NA	NA
PSKPI-04: User density	0.05	devices/m2
PSKPI-05: Video resolution	60-144	fps
PSKPI-06: Application service creation	<5	min
PSKPI-07: Network Applications deployment time	<5	min
Energy saving	~30	%

9.6 KVIs

The following table maps the minimum set of KVIs to be evaluated within the context of UC6 in relation to FIDAL objective:

Table 40: KV's of initial potential relevance for UC6.

Key Value Theme	UC6 - XR-assisted services for public safety
Democracy	
Trustworthy	Dependability (uninterrupted, high-quality service)
Inclusiveness / Equal Opportunity	Accessible, available, and cost effective for all PPDR users
Fairness	Lack of bias in how medical professionals can assess
Personal freedom	dignity for patients and medical professionals
Transparency	Understandability, justifiability
Privacy	Privacy preserving for patients and medical professionals
Economic Ecosystem (part of sustainable 6G)	
Business Value	Decreased cost and time to engage with service, production of business plans
Tackling economic inequality	Output relevant to all socio-economic demographics; training opportunities
Innovation	
Responsibility	Existence and effectiveness of risk management oversight; enables alternative approaches
Open collaboration	Improved awareness among partners of users values, challenges, and needs; participatory processes
Flexibility	Optimal resource allocation
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Reduced energy consumption, environmental footprint
Waste Management	Increased lifespan
Safety and Security	
Safety	provide advanced surgical services for urgent incidents
Security	Security preserving, vulnerabilities mitigated
Data protection	Sensitive data protected
Societal Ecosystem (part of 6G for sustainability)	
Healthier community	Access to medical services
Knowledge	The connection of diverse technical and skill groups will increase knowledge and skill acquisition

10 UC7 – Smart village engagement services

10.1 Scenarios, contexts, and workflows

There is a need to assign an enhanced media-enabled citizen engagement service to a high number of end-users and equipment for city planning and operation of welfare services across different operators and domains. Current specialised citizen services and applications are poorly enabled, due to lack of support of managed network and QoS connectivity. Security requirements or adequate protection of privacy for citizens are not catered to, and separate networks are not cost-efficient. Two scenarios are relevant for the UC 7:

- **UC scenario #1: Co-created engagement in urban communities**
- **UC Scenario #2: Co-created engagement in rural areas**

The illustration in Figure 15 below illustrates the opportunities real-time VR features can play in both scenarios 1 and 2. The UC scenarios are elaborated below.



Figure 15: Stakeholder (citizen or city/rural community official) operating on digital twins and real time coordinating of incidents in rural areas using VR capabilities.

10.1.1 UC scenario 7.1: Co-created engagement in urban communities

Citizen engagement implies involvement from the citizens in the city's decision-making processes addressing their and society's needs. Citizen engagement can take different forms such as co-design and co-creation of urban interventions to submitting suggestions and initiatives to municipalities. With VR capabilities citizens can interact with municipality representatives real time or through accessing and editing digital twin features of the city while performing inspections and city walks. This use case scenario also includes artistic co-creation, e.g., music and performing arts across domains in the community. This use case supports two of the UN's sustainable goals, #9 Industry innovation infrastructure and #11 Smart sustainable cities [2].

10.1.2 UC scenario 7.2: Co-created engagement in rural areas

Bridging the digital divide between urban and rural areas is necessary improving both the primary and service industries as well as public sector as well as the quality of life for the citizens. In remote operation and emergency situations as well as management of infrastructure crises and disasters there is a need for a reliable network with

features that supports real time communication, situational awareness (e.g., using VR headsets) for coordination of private and public resources involved. This use case supports the long-term strategy of the European Commission for how connectivity can revitalise local communities and make them more sustainable [3].

10.2 Stakeholders

10.2.1 Stakeholders' identification

All the stakeholders involved and/or can benefit by the implementation of the use case:

- Scenario 7.1: Involves citizens, city authorities and representatives from sectors in municipality, application providers and equipment vendors, technology and network provider etc.
- Scenario 7.2: Involves stakeholders from the primary and service industry, as well as public stakeholders such as emergency/Blue light services (Health, Fire, Defense, Police).

10.2.2 Stakeholders' benefits

Stakeholder benefits are found in the two scenarios, The latter also specify network operator benefits.

- Scenario 7.1 - 5G enables benefits for the city officials is reduced costs from less failure area planning. Shorter development time for innovative solutions on city challenges/area planning 5G enabled benefits for the citizens and easy and cost-efficient VR/AR remote maintenance/mission critical services. Faster development time and less failings from digital twins' pilots.
- Scenario 7.2 - Revenues from connectivity, platform management and integrated solutions are relevant benefits for network provider. The municipality is also highly relevant beyond the core value chain stakeholders, improving the capabilities for crisis management throughout the community/region. Beyond 5G will enable the network operator to better serve differentiated use case requirements more cost-efficiently. Moreover, being able to scale and develop standard templates for 5G advanced services and ensure service availability/SLA levels across multiple service and user types as agreed under congested or faulty situations.

10.2.3 Stakeholders needs

Stakeholder needs are found in the two scenarios.

- Scenario 7.1: Today's citizens' pain points are quick collecting and analysing planned city development effects virtually as well as insights into citizens demands and partner requirements. For application providers there is a lack of data available and large-scale testing with pilot cities/citizens. Constraints are lack in real time data for city assets, buildings, bridges, towers, dams etc. Using current 5G mobile communication is challenging (latency and throughput time) for real time handling.
- Scenario 7.2: Today digitalisation of rural areas is not mature enough to realize this use case now. Moreover, the current fifth generation mobile technology (5G) are challenging with respect to latency and throughput values for real time information and interaction.

10.3 How can beyond 5G networks benefit the UC

If citizen engagement services could be managed cost-efficiently with sufficient levels of security, it would increase public capability for large scale engagement with citizens and increased level of citizen engagements in city (service) developments. Beyond 5G will introduce new terms of service or new technology with respect to state of the art and similar behaviour currently available.

- Scenario 7.1: VR and real time co-creation features for urban communities, digital twins. Joint development on digital platforms/digital twins and open public data for brainstorming and piloting proof-of concepts while other municipalities exploring usage of AR/VR in in area planning and dialogue with inhabitants.
- Scenario 7.2: VR/AR enhanced supervision/operation for mission critical services (fire, police emergency teams etc.) in rural areas. Drones with 5G network antennas and video cameras distributing real time pictures and videos of the situation to emergency personnel involved.

10.4 Technology needs

The use case will explore how to set up many services and applications with logical network (as a Service, LNaaS) contracts to be mapped onto one or a few 5G network slice instances, i.e., the large-scale trial will explore putting up many connectivity contracts (LNaaS SLAs, serving multiple users, devices, and application types) for customers and



their media applications with varying QoS, served by many different configurations of network slices. UC7 can be seen as an extension and continuation of UC5 where an important technological extension of the test-bed facility will be for enabling and supporting digital twin facilities. This includes extensions in the edge cloud to add relevant compute resources, orchestration, and management. UC application-level support by operational tools, e.g., for handling SLA provisioning and management, including QoE related support. With this in mind we refer to UC5 Technology needs above for this release while the next release of this deliverable will go into more depth of technology needs for UC7.

10.4.1 5G services needs

For further study. See also above.

10.4.2 Network Application needs

For further study. See also above.

10.4.3 Equipment needs

For further study. See also above.

10.5 KPIs

The following table presents a list of indicative targets technological KPI values for UC7. While these KPIs can be considered as target KPIs under excellent conditions we will also investigate elasticity of the KPIs in the context of different applications and their use case scenarios, exploring also when KPIs can be considered as “passed”, “partially passed” and “not passed”.:.

Table 41: Target technological KPIs for UC7.

Key Performance Indicators (KPIs)	Value	Units
MSKPI-01: App/Server Accessibility	100	%
MSKPI-02: Content Load time/time to first picture	0.1	sec
MSKPI-03: Content Stall/Freeze	0	%
MSKPI-04: Content Download Throughput	20	Gbps
MSKPI-05: Content Upload Throughput	5	Gbps
MSKPI-06: Application service creation	<5	min
MSKPI-07: Network Applications deployment time	<5	min
Network Latency (multiple cases)	TBP	ms
Throughput uplink (multiple cases)	TBP	Mbs
Throughput downlink (multiple cases)	TBP	Mbs
E2E Audio QoS (multiple cases)	TBP	Mbs, loss, latency, jitter
E2E Video QoS (multiple cases)	TBP	Mbs, loss, latency, jitter
App/server Accessibility (service availability, multiple cases)	TBP	%
Network App deployment and provisioning (multiple cases)	TBP	Minutes
Service / SLA provisioning time (multiple types of services)	TBP	Seconds
QoE (multiple user contexts)	TBP	MOS
Measure on resource utilization	TBP	TBP
Measure on utility efficiency	TBP	TBP

10.6 KVis

The following table maps the minimum set of KVis to be evaluated within the context of UC7 in relation to FIDAL objective:

Table 42: KV's of initial potential relevance for UC7.

Key Value Theme	UC7 - Smart village engagement services
Democracy	
Trustworthy	Dependable, consistent, building confidence
Inclusiveness / Equal Opportunity	Service access and availability, local skill creation
Fairness	Fair distribution and access to public services and decision-making
Personal freedom	Ability to choose when to join in to such activities, dignity
Transparency	Auditability, understandability, explainability, justifiability
Privacy	Privacy preserving, support individual expression and right to assembly
Economic Ecosystem (part of sustainable 6G)	
Economic Sustainability	Improved opportunities for local communities, market impact, engaging legacy systems, improved business access to supply chain
Business Value	Perception of problems solved, business plans
Tackling economic inequality	Output relevant to multiple socio-economic demographics, improved local business opportunities
Innovation	
Responsibility	All parties able to assess responsible use of the system
Open collaboration	Collaborative and participatory methods to understand how connectivity can improve services and experiences
Flexibility	Work in different environments and scales
Environmental Ecosystem (part of 6G for sustainability)	
Environmental Sustainability	Decrease energy and resource use through digital connections, if new energy use is proportionate
Waste Management	Decrease waste through improved potential for virtual connection, re-use of existing devices/architecture
Mitigation Strategies	Improved environmental monitoring of tools in ways that support stakeholders in developing mitigation strategies
Compliance Quality Standards	Working with compliance quality standards can support stakeholders in their own environmental assessments
Safety and Security	
Safety	Improved community safety, easy to use tools
Security	Decreased vulnerabilities; delegation of responsibilities
Data protection	Personal data protected with user control.
Societal Ecosystem (part of 6G for sustainability)	
Societal sustainability	Increased opportunity for stakeholders of all type to participate, collaborate, create, and have a voice in their communities; diverse representation in use cases, gender equality
Healthier community	Improved relationships with organisations, people satisfied with where they live
Cultural connection	Improved access to public services, community culture, sense of community, wide variety of cultural domains impacted
Knowledge	Enhanced digital literacy
Quality of Living / Wellbeing	Improve mental and social contentment

11 Requirements elicitation via Focus Groups discussion

The FIDAL requirement elicitation methodology was based on a discussion within Focus Groups; each group maps to an already identified project stakeholder category. A Focus Group generally consists of a small group of partners, who are brought together, in a moderated discussion focused on a given issue or topic, aiming to explore attitudes, perceptions and ideas about a topic³³. This approach was favored over the more conventional approach of soliciting requirements from partners individually or via questionnaires, as Focus Groups allow individuals to interact with each other, resulting in the generation of insights that would not otherwise be accessible. Partners were classified into the following groups based on their profiles, and their participation in the relevant project tasks:

- Infrastructure owners: NOVA, IQU, TNOR, PNET, TID, UMA.
- Owners of Use Cases and Network Apps: FORTH, EKT, ADS, STWS, OWO, ORAMA.
- Open Calls stakeholders: PNET, NOVA, UoP, PIU.
- Experimenters: FORTH, EKT, ADS, STWS, OWO, ORAMA, IQU, ISI, UBI, APART.

The Focus Groups discussion took place virtually via teleconferencing and was split into 2 sessions, which addressed Focus Groups 1-2 and Focus Groups 2-3 respectively. One facilitator guided the discussion while also taking notes of user needs, which were encoded in Table 43.

Table 43: Table of User Requirements.

UR1	Service Orchestration
The FIDAL facility should support orchestration of testbed services, via service management APIs exposed by the testbeds	
UR2	Slice Orchestration
The FIDAL facility should offer a slice orchestration service, via slice management APIs exposed by the testbeds.	
UR3	Testing as a Service (TaaS)
The FIDAL facility should provide TaaS capabilities. Mature experimentation tools already supported by the FIDAL testbeds are securely exposed to experimenters via a single-entry point or portal.	
UR4	Data Collection
The FIDAL framework offers data collection services, to be used during trials execution as well as open calls experiments. For this reason, testbeds expose telemetry APIs.	
UR5	Repository Services
The FIDAL system offers repository services, for storage of artefacts, ...	
UR6	Zero Touch Management
The FIDAL framework must offer Zero Touch management of facilities	
UR7	Reservation of experimentation slots and resources
FIDAL should offer adequate resources and the capability to reserve them for the execution of UC trials and Open Calls at the project testbeds	
UR8	Scheduling of Open Calls Experiments
FIDAL should offer administrative support to Open Calls participants, to help them schedule their experiments in a way that avoids resource conflicts	
UR9	Feasibility Check of Open Calls experiments
FIDAL should perform a feasibility check of the open calls experiment requirements, to establish if they can be deployed at existing testbeds	
UR10	Network Applications Catalog

³³ Robinson, J. (2020). Using focus groups. In Handbook of qualitative research in education. Edward Elgar Publishing

FIDAL offer a catalog service, facilitating the storage of Network Applications' images, metadata, and requirements that can be shared across testbeds (and be exposed to third parties?) and queried by experimenters.	
UR11	Network Applications Ordering and instantiation
FIDAL allows the ordering and dynamic instantiation of Network Applications stored at the catalog, at testbed infrastructures	
UR12	Inventory Runtime Information for Network Applications
Information regarding the status and other runtime information of instantiated Network Applications can be offered on demand	
UR13	Experiment Triggering
Experimenters internal and external to the project (i.e., via open calls) can trigger an experiment via the TaaS provisions offered by the testbeds	
UR14	Experiment Results
FIDAL will provide a solution for system-wide data collection and visualization. Experimentation results are collected from all testbeds and visualizations are provided to the experimenter on demand	

12 Agile User Stories

In order to better capture the envisioned functionality of the FIDAL system, the User Requirements were represented as Agile user stories and mapped to the project stakeholders. A user story is a general requirement presented from the perspective of the user^{34 35}. The User Story is a well-established method for expressing requirements in modern requirements elicitation approaches. For this reason, we also adopted it in our methodology for the FIDAL requirements elicitation. In the current document, the template that is used to write the user stories and that is adapted³⁶ is the following:

As a [persona], [name] [wants to] [so that]

For each user story, a table featuring the following attributes is provided:

- <StnoSTno>: The first “Stno” refers to the number of the stakeholder and the second “Stno” relates to the number of the story.
- Goal: This refers to what how the stakeholder wants to interact with the platform.
- Acceptance criteria: This refers to what the system should do to be accepted by the user.


User stories have been created for each of the four main categories of stakeholders who will interact with the FIDAL Experimentation Facility. In addition to the user stories, user personas have been created. User personas are an indispensable part of the Agile approach, since characteristics representative of a group of people assist product teams in understanding their target audience³⁷.

The agile requirements elicitation was based on discussion during the focus groups that provided information and helped in defining what stakeholders expect from the FIDAL Experimentation Facility. The user stories for each stakeholder (Stakeholders from the media and PPDR sector, Developers of Network Applications, Telecom Operators, Testbed owners) are provided in Section 13. In the next subsections, for each tracked stakeholder, a few user stories are described to reflect the URs from the FIDAL facility.

12.1 Infrastructure owners’ User Stories

Infrastructure owners are legal entities that own the platform as well as the included tools and they are accountable for managing the testbed resources. A user persona of this group and the user stories are presented in Table 44 and Table 45.

Table 44: Infrastructure owner Persona.

	<p>BIO Paul is a 51 years old staff for a multinational telecommunications company that has been operating for more than 20 years. He has an MSc in Computer Engineering and Informatics. Among his responsibilities is the management of the testbed facility that is owned by the company. Currently, he is a pursuer of network solutions for new media applications.</p> <p>Goal: accommodate the building of Network Applications and testing of media applications.</p> <p>Challenge: lack of technology to meet and support different needs</p>
--	---

³⁴ Rehkopf, M. (n.d.). User stories with examples and a template. Atlassian. <https://www.atlassian.com/agile/project-management/user-stories>

³⁵ Agile Business Consortium. (2014). The DSDM Agile Project Framework Handbook. <https://www.agilebusiness.org/page/TheDSDMAgileProjectFramework>

³⁶ Rehkopf, M. (n.d.). User stories with examples and a template. Atlassian. <https://www.atlassian.com/agile/project-management/user-stories>

³⁷ Faller, P. (2019, December 7). Putting personas to work in UX design: what they are and why they’re important. Adobe. [https://xd.adobe.com/ideas/process/user-research/putting-personas-to-work-in-ux-design/#:~:text=What%20is%20a%20user%20persona,see%20in%20the%20example%20below\).](https://xd.adobe.com/ideas/process/user-research/putting-personas-to-work-in-ux-design/#:~:text=What%20is%20a%20user%20persona,see%20in%20the%20example%20below).)

Table 45: Infrastructure owner user stories.

ST1ST1	
Goal	As an Infrastructure Owner, Paul wants to facilitate network management automation and slice orchestration so that guarantee advanced testbed services to their customers.
Acceptance Criteria	<ul style="list-style-type: none"> The platform should provide service and slice management APIs exposed by testbeds. The platform should provide zero-touch management services.
Relevant Requirements	UR1, UR2, UR6
ST1ST2	
Goal	As an Infrastructure Owner, Paul wants to ensure the provisioning of TaaS capabilities so that allow experimenters trigger an experiment.
Acceptance Criteria	<ul style="list-style-type: none"> The platform should provide access to TaaS via a single-entry point or portal. The platform should provide mature tools for experimentation.
Relevant Requirements	UR3

12.2 Use Case and Network Application owners' User Stories

They are the people/companies that provide foundational services for the media industry. They constitute one of the three main categories of customers. Network Applications developers will be able to use the FIDAL Experimentation Facility with the aim of designing and building their Network Applications by having access to a wide range of resources through the Network Applications Repository, which means that they will use the Experimentation Facility as a PaaS. Also, they will have the opportunity to test the Network Application they develop, thus taking advantage of the TaaS offerings of the Facility. Table 46 and Table 47 present a user persona of this group and the respective user stories.

Table 46: Network Application developer persona.

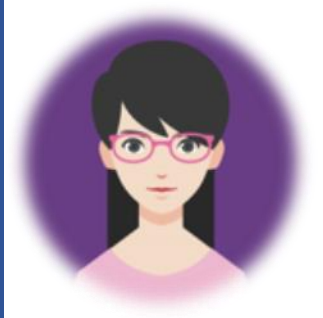
	<p>BIO Angela is a 29-year-old with MSc in computer science. She works as a freelance Network Applications developer with numerous technical skills and experience more than 8-years. She is passionate with the creation of Network Applications which she can make available to other Network Applications developers.</p> <p>Goal: develop, test and publish Network Applications</p> <p>Challenge: lack of 5G experimentation platforms for developing and onboarding Network Applications</p>
--	---

Table 47: Network application developer user stories.

ST2ST1	
Goal	As a Network Applications developer, Angela wants to be able to manage her Network Applications so that she can successfully (re)use and validate them.
Acceptance Criteria	<ul style="list-style-type: none"> The platform should provide a catalogue service in order to facilitate the storage of Network Applications' images, metadata, and requirements that can be shared across testbeds (and be exposed to third parties) and queried by experimenters. The platform should allow the ordering and dynamic instantiation of Network Applications stored at the catalogue, at testbed infrastructures.

	<ul style="list-style-type: none"> The platform should offer on demand information about the status and other runtime information of instantiated Network Applications.
Relevant requirements	UR10, UR11, UR12

12.3 Open Calls Stakeholders' User Stories

Open calls are related to entities that use the platform tools to execute experiments and develop applications to integrate their solutions.

A user persona of this group and the user stories are presented in Table 48 and Table 49.

Table 48: Open call Participant Persona.

	<p>BIO Mike is a 42 years old staff for a multinational telecommunications company that has been operating for more than 20 years. He has an MSc in Computer Engineering and Informatics. Currently, he is a pursuer of efficient network solutions for new media applications.</p> <p>Goal: testing and validation of media applications</p> <p>Challenge: lack of technology to meet and support different needs</p>
---	---

Table 49: Open Call Participant User Story2.

ST2ST1	
Goal	As an Open Call participant, Mike wants to bind a testbed and resources so that he can execute an experiment without resource conflicts.
Acceptance Criteria	<ul style="list-style-type: none"> The platform should be able to administer the experiments scheduling allowing Open Call participants to reserve the preferred time slots and required resources. The platform should provide feasibility check namely to detect the allocated resources and the adequacy of testbeds to support the requirements of Open Calls experiments (or UC trials).
Relevant Requirements	UR7, UR8, UR9

12.4 Experimenters User Stories

The stakeholders in this category are people/companies from Media and PPDR who will use the facility to test their applications in a 5G environment using the FIDAL Experimentation Facility "TaaS". Hence, these people occupy the role of the "Vertical Tester" or else "Experimenter" when they interact with the platform.

A user persona of this group and the user stories that have been identified are presented in Table 50 and Table 51.

Table 50: Experimenter's persona.


	<p>BIO Bob is a 37-year-old production services director in a company that provides 3D graphics and XR/VR-assisted services for public safety. Currently, he is interested in developing products for other sectors, such as the industry, educational sector.</p> <p>Goal: test the immersive experience of being in a XR/VR environment</p> <p>Challenge: lack of 5G technologies and lack of knowledge of 5G networks</p>
---	---

Table 51: Experimenter's user story.

ST4ST1	
Goal	As an experimenter, Bob wants to have access to TaaS using the provisions offered by testbeds. so that he can execute his experiment in a 5G environment.
Acceptance criteria	<ul style="list-style-type: none"> The platform should allow via open calls internal and external experimenters trigger an experiment.
Relevant requirements	UR13
ST4ST2	
Goal	As an experimenter, Bob wants to collect and storage artefacts (experiments data, training sets, etc) so that they can be reused, self-managed and controlled.
Acceptance criteria	<ul style="list-style-type: none"> The platform should offer telemetry APIs (exposed by testbeds) to allow data collection during UC trials execution and open calls experiments. The platform should provide a solution for system-wide data collection and visualization. The platform should provide to the experimenter on demand collection of the results from all testbeds and visualizations.
Relevant requirements	UR4, UR5, UR14

13 Overall architecture

13.1 Logical architecture of the FIDAL framework

The following figure presents an overview of the logical architecture, which consists of the FIDAL components and their corresponding interfaces.

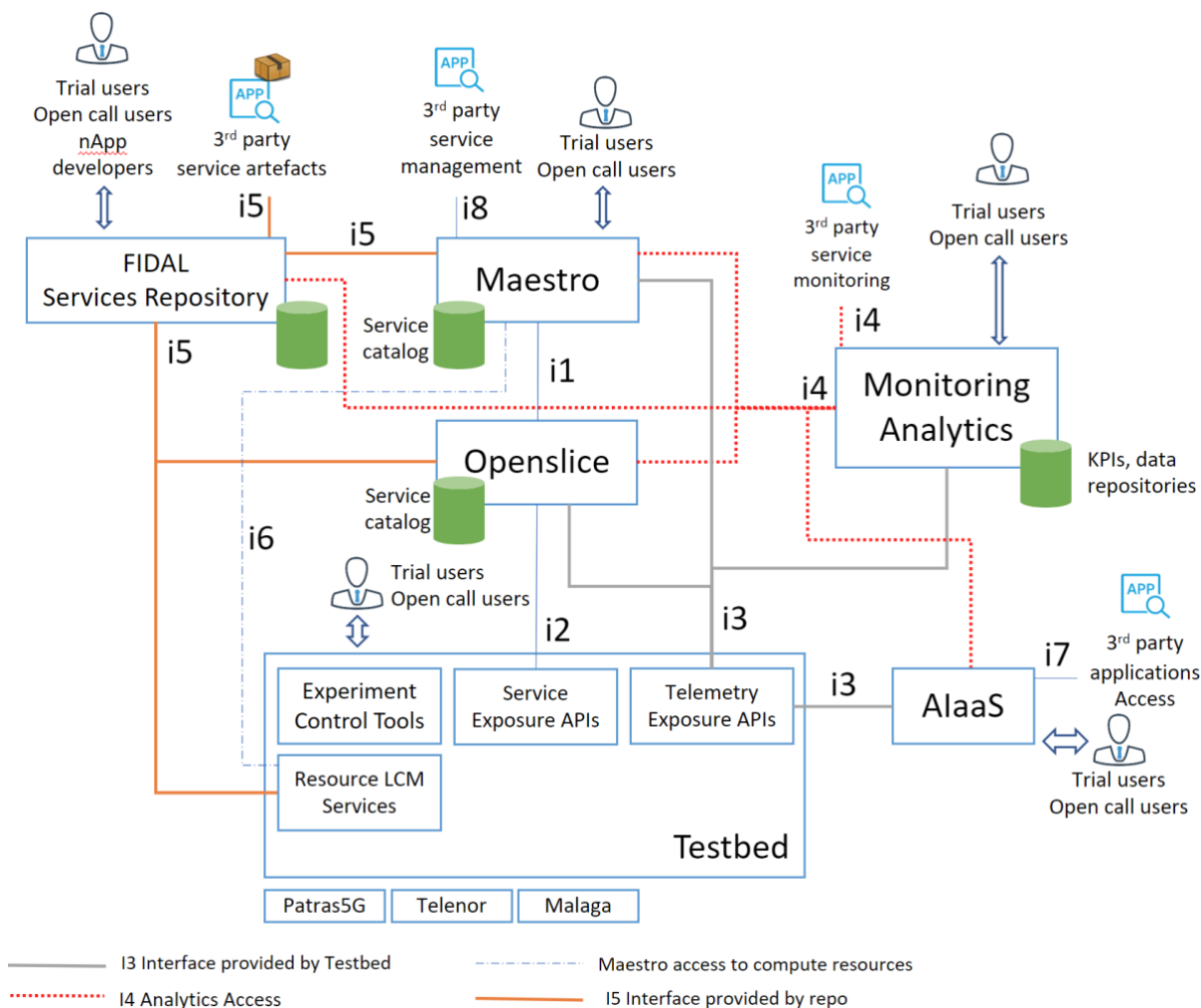


Figure 16: : FIDAL Logical Architecture Diagram.

The architecture has been designed to deliver an end-to-end infrastructure that is scalable, flexible, and efficient, leveraging the latest advancements in beyond 5G technologies and research. The primary components that facilitate network management automation and slicing orchestration are Maestro and OpenSlice, which will be deployed at a centralised location at Patras5G-PNET premises, along with all monitoring and analytics tools. A FIDAL repository will be hosted at an ATHENA's server while Telenor and Victoria testbeds will be deployed at their respective sites, connected, and configurable through exposed APIs, allowing secure remote access.

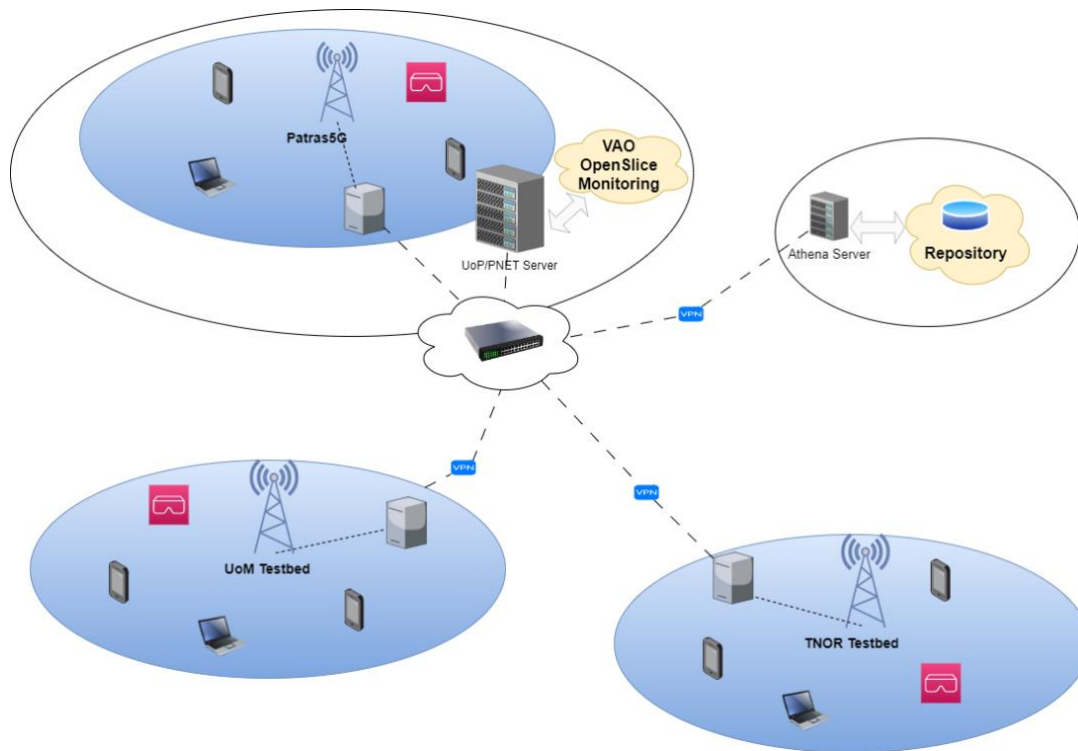


Figure 17: FIDAL's Deployment plan.

All FIDAL end users will have access to available services and experimentation tools from MAESTRO and each testbed respectively. They will also have the capability to browse network applications from the FIDAL repository and retrieve and visualise their results from the monitoring analytics framework. A high-level description of each component's role within the logical framework is presented next.

i. MAESTRO

Maestro is a service orchestration platform designed atop Infrastructure as a Service (IaaS) and Platform as a Service (PaaS) cloud environments. FIDAL applications are onboarded through Maestro's user interface (UI) or a northbound service onboarding API, both following TM Forum's service specification APIs. To deploy FIDAL application atop certain infrastructures, Maestro interfaces with the Openslice OSS through an internal API (i1). Maestro is described in detail in Section 14.1.

ii. OpenSlice

Openslice will be used as FIDAL cross domain slice manager to enable the seamless onboarding and provisioning of network applications as well as to orchestrate the network services involved in the large-scale trials. It interacts with Maestro through an internal interface (i1) and translates application requirements into concrete computational, networking, and storage resources across the various domains that it manages. Openslice is described in detail in Section 14.2.

iii. Monitoring Analytics

The scope of Monitoring analytics is to collect and homogenise data, produce respective KPIS and to produce the means to visualise the metadata through a user portal. Monitoring tools are interconnected through interfaces with OpenSlice, Maestro, and the FIDAL testbeds, gaining access to raw metrics from network applications, testbeds and other user equipment and exporting the analytics to visualization portals. The main subcomponents of the monitoring platform architecture are:

- Data collector;
- Internal database;

- KPI modeler;
- Internal REST API;
- Visualization Portal.

All subcomponents are described in detail in Section 14.4.

iv. AI as a Service (AlaaS)

AlaaS is perceived as a standalone component that would produce knowledge based on any metrics, telemetry, and monitoring data from sources such as the OSS, the NFVOs and the cloud infrastructure. It will be developed in such a way to provide intelligence on decision making on the orchestration level, the runtime adaptations, and the underlying infrastructure. To integrate AI as a service block into the architecture, bidirectional interfaces (i.e., i4 to harvest data from monitoring analytics, Maestro, and OpenSlice, and i8 to serve the results of the AI models targeting different objectives and SLAs) are essential, one with the testbeds and one with the underlying and internal services of the infrastructure. Control loops based on monitoring data can be dynamically reconfigured based on AI decision making. AlaaS is described in detail in Section 14.3.

v. FIDAL Repository Services

The FIDAL Repository Services' main purpose is the collection and dissemination of the test artifacts, with a supplementary role supporting internal functionalities such as API and network application reusability. Reusability of repository resources by testbeds, OpenSlice and Maestro can be achieved through dedicated interfaces (i5 to i7). The architecture of the repository will include a catalogue of available Network Applications, AI models and project outcomes. FIDAL repository services is described in detail in Section 14.5.

vi. FIDAL Testbeds

The block describing the functionality of a FIDAL testbed includes four subcomponent blocks, namely an experiment control tools, the service exposure APIs, the telemetry exposure APIs and the resource lifecycle management (LCM) services. Trial and open call users can interact directly with the testbed and request services and experimentation tools that are available. All testbeds will expose APIs and via interfaces (i2 and i3) will allow the orchestration of network services by OpenSlice slice manager and processing of telemetry data by the monitoring analytics framework (chain block). Each testbed will be remotely connected to the repository and could reuse any of the available resources (e.g., docker image) from the FIDAL platform.

vii. Network Applications

FIDAL adopts the Network App (Network Applications) concept, first introduced in the E.C. Innovation Action of Horizon 2020 5G-PPP Phase 3b ICT-41 program, as a as a middleware layer that serves vertical applications. In particular, Network Applications expose reusable functions (e.g., VR content Streaming) to vertical applications via open Northbound APIs. Network Apps are key drivers for drastically reducing service creation time, therefore making 5G and Beyond networks attractive for SMEs. FIDAL considers them key in the future 5G evolution towards 6G and plans to pave the way for Beyond 5G Network Apps, while adopting modern Cloud-Native technologies (i.e., Containers, Kubernetes, and Helm charts). The FIDAL Network Applications are implemented as cloud-native backend services deployed within k8s clusters inside the project testbeds and orchestrated by MAESTRO (see Section 14.1) and are accessible by UEs via the respective 5G network. Their Northbound APIs are typically consumed by frontend components and / or external Tenant Platforms (e.g., cloud servers), and can be made available to future open calls that may implement Over the Top (OTT) functionalities. They may also interact with the 5G System (5GS) via 3GPP standard-compliant interfaces (e.g., the N5 interface which allows Network Apps to perform end-to-end 5G QoS modification and control). Other control-plane 5GC functionalities accessible to Network Applications are:

- To Trigger UE actions (UE activation, feedback message, etc.),
- To retrieve event notifications (e.g., loss of UE connectivity),
- To Retrieve network analytics,
- To configure network parameters (e.g., routing).

FIDAL Network applications represent the two vertical domains addressed by the project (i.e., Media and PPDR). FIDAL Network Applications, to be detailed in D3.1, are summarised in Table 52.

Table 52: List of FIDAL Network Applications.

Network Apps table		
Name	Description	FIDAL Partner
MCX Network App	The Mission Critical Multimedia Communication and Collaboration, so called MCX, is a End2End solution, that implements the MCX services standardized in 3GPP (Push-To-Talk - MCPTT, Mission Critical Data – MCDData, Mission Critical Video - MCVideo services)	ADS
StreamSelector Network App	StreamSelector offers a low latency video gateway with video processing capabilities, acting as a networked video switching matrix. It establishes connection between video sources and video destinations	EKTA
Remote XR Render-Streaming Network App	Remote XR Render-Streaming network application will scale the XR Unity Rendering pipeline to cloud/edge resources, away from the user equipment (UE), facilitating advanced processing capabilities with low latency that reduce the imposed constraints on limited resources, GPU, battery, and mobility on untethered head-mounted displays (HMDs).	ORAMA
Remote Sensations Network App	This Network app offers a solution that allows to send real physical sensations through 5G during police training sessions. Before sending the sensations, the user will need to go through a login process and, once it is successful the Network App will be available to receive and manage the sensation the user must feel from the VR Headset. After processing, the sensation command will be sent to the OWO App which communicates with the OWO Vest and will apply on it the sensation configured on the Network Application.	OWO
Remote scene analysis and AR annotation Network App	This Network App provides real-time annotations on the agents' AR devices (Head Up Displays – HUDs), as they have been identified by the rapid scene analysis Network App. In detail, this Network App offloads the intensive process of analysing the video captured by the agents' HUDs to edge devices enabling this way the employment of advanced Machine Learning algorithms for person and object detection and tracking.	FORTH
AFD Network App	The AFD Network App enables the detection of major wildfire incidents. Camera feeds will be provided to the service, enabling the analysis and automatic fire detection, providing to the clients the related fire detection alarms	SWTS

viii. Interfaces

The interfaces previously noted in **Error! Reference source not found.** which shows FIDAL's logical architecture, are listed and briefly described in Table 53.

Table 53: FIDAL architecture interfaces and APIs.

Interface-ID	Related Modules	Type	Description
i1	Maestro, Openslice	Service management API	It is the exposed API from Openslice. TM forum API based to create/order services and network slices. See the related section on Openslice
i2	Openslice - Testbed	Slice management API	This is exposed by the testbeds and specifies their slice management APIs. Openslice mainly consumes this interface

			towards the testbeds. For more details of this exposure see the next section of the FIDA testbeds architectures
i3	Mestro Openslice, Monitoring Analytics, Testbed, AlaaS,	Telemetry and monitoring API	Testbed exposed APIs (e.g. Prometheus) for telemetry and monitoring data consumed by Monitoring Analytics, Openslice, Maestro and AlaaS
i4	Monitoring analytics, Maestro, Openslice, AlaaS, Repository Services	Data collection API	Monitoring Analytics exposed API. Can be consumed by Maestro, Openslice, Repository Services and AlaaS. Can be consumed also by 3 rd party applications
i5	Testbed, Repository	Repository catalog API	A set of APIs (resource catalog API, image registry API) exposed by FIDAL repository services, that enables the reuse of network applications and any other available resources (images, files, etc.) Can be consumed by Maestro, Openslice, Testbed LCM services (e.g. OSM, Kubernetes).
i6	Maestro, testbed Resources	Services LCM	Mestro needs to (re)-configure deployed applications after the network slice is created. This is achieved over this interface
i7	AlaaS	AI API services	This interface exposes APIs of the AlaaS, for example Dedicated RESTful endpoints for serving AI/ML models via open data exchange standards
i8	Maestro	Service exposure	API exposed by Maestro to be consumed bby 3 rd party applications and services. For more details see the Maestro section

13.2 Physical architecture of the FIDAL facility

13.2.1 Patras5G Testbed

The Patras5G/PNET testbed consists of an open infrastructure acting as an isolated private infrastructure for 5G and IoT applications. The infrastructure components are based on both open-source and commercial solutions, with dedicated components and services for 5G and IoT scenario deployments. The testbed supports both containerized and virtualised deployments from 5G RAN to 5G Core including 5G standalone (SA) setups, an AI dedicated Kubernetes cluster with NVIDIA GPUs, a 400Gbps network based on P4 switches, as well as the necessary cloud and SDN fabric to host any service that needs to be tested and integrated with the testbed infrastructure. Access to users and applications is enabled by the open-source Operations Support System (OSS) Openslice.

The testbed supports testing and experimentation in a private 5G Network with standard-conformant components and core network infrastructure, operated in licensed and unlicensed spectrum, with our own SIM cards. A mmWave backhaul is installed to various locations in the city of Patras to link the access to the core network, and Fixed Wireless Access to provide broadband services to the facility and there is Integration of various open source and commercial 5G Cores with SDR platforms and UEs and g/eNB. MEC orchestration and mobility management features are supported for interactive mobile streaming edge services. Most of the installed components are offered as Open Source but there are also dedicated components and services to support 5G and IoT scenarios.

PNET/NOVA pre-commercial 5G extension: The testbed hosts a 5G pre-commercial site, based on ERICSSON 5G equipment. It comprises from several 5G radios and a dedicated UPF, while the 5G Core is co-located remotely in Athens containing all related functions (AMF, SMF, NEF, etc) by NOVA which provides a dedicated slice for PNET. This

extension offers a unique opportunity to test 5G/6G cloud to edge scenarios as well as various non-public-network deployments. The pre-commercial network extension is illustrated in Figure 18.

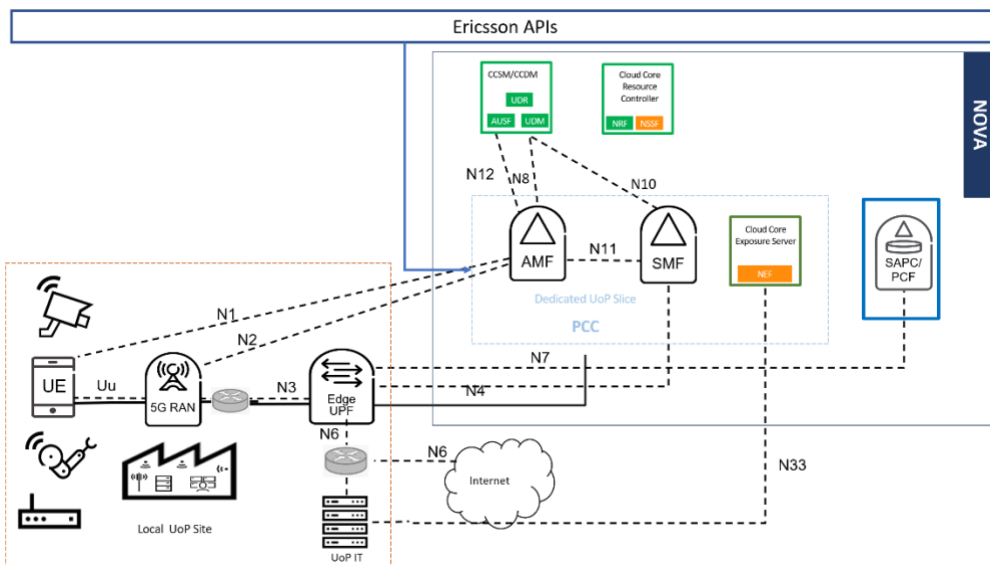


Figure 18: PNET/NOVA pre-commercial network extension.

Vertical applications can access the Patras 5G Service Catalog, self-manage and onboard their artefacts through a web portal or access programmatically available services. Various artefacts can be managed through APIs via standardised TMForum OpenAPIs: Service Catalog, Service Order and Service Inventory, Partner Management and Users, Service Orchestration, VNFs/NSDs Catalog, NFVO endpoints via OSM NBI, Service and NFV Deployment requests. The testbed provides monitoring data and metrics related to the Cloud infrastructure, for all the VNFs and all the RAN nodes via NetData, as well as measurement sensors for Energy consumption of compute nodes, switches, 5G gNBs and CPEs while all data are gathered in a Prometheus server. A Prometheus as a service within a slice is also available. We are also developing our own NWDAF for analytics. In Figure 19, a diagram with the Patras5G architecture is presented.

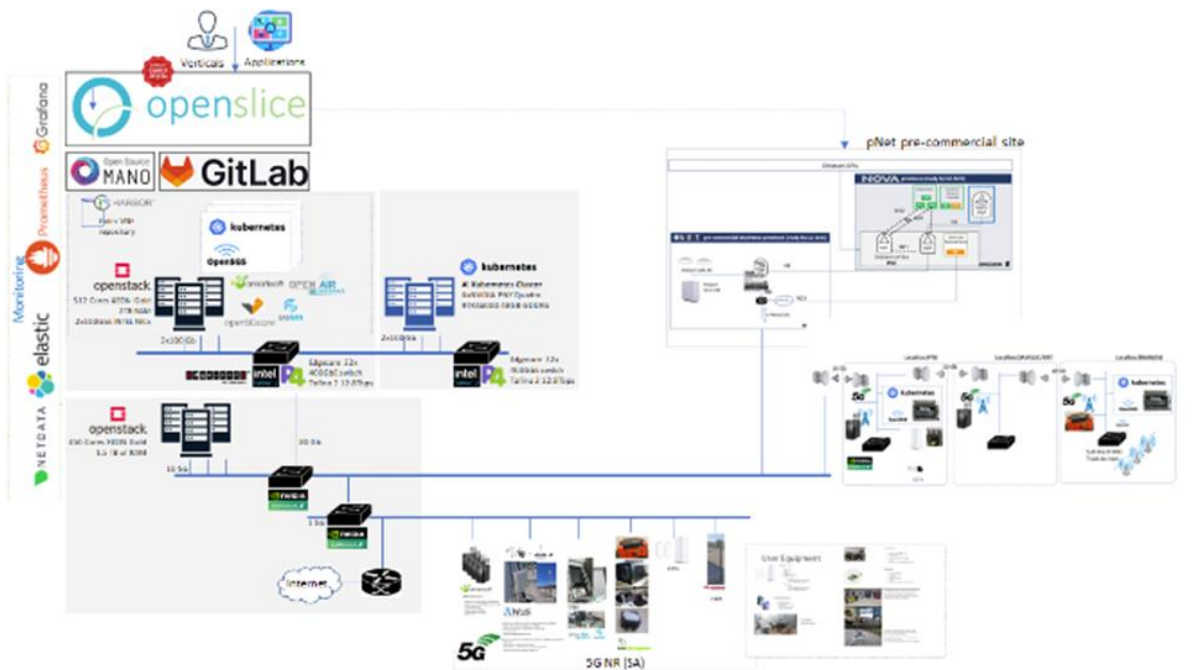


Figure 19: Patras5G Architecture diagram.

13.2.2 Victoria Network Testbed

UMA is operating an infrastructure called Victoria Network. The infrastructure is devoted to research in 5G and beyond 5G technologies and uses cases combining commercial carrier-grade and open-source network components. The indoor setup is based on a Keysight emulator for 4G and 5G, plus anechoic chambers, commercial user devices, and advanced monitoring equipment (energy, spectrum, etc.). Currently, emulators support frequency bands from 800MHz to 26GHz. The outdoor deployment is based on a collaboration with Telefonica, with NOKIA cells on the Malaga university campus. These cells are connected to local core networks to provide a fully private network. They support LTE and 5G NR to implement the Non-Stand-Alone and Stand-Alone modes. The distributed configuration with base unit plus remote heads allows it to move towards a C-RAN deployment. The support of several network identifiers (PLMNs) with MOCN technologies is used to implement a first level of slicing at the radio, offering up to six operators simultaneously. On top of that, ITIS has obtained authorisation to use 26 GHz band for a millimetre wave. The virtualized infrastructure with support for traditional virtual machines and containers supports any approach to service deployment. This setup is expanded to the city centre through an agreement with Malaga, Malaga Harbour, and Torremolinos. Finally, two new 5G private deployments will be connected to the Malaga university campus deployment. These new deployments are located at La Mayora experimental station and the test track for autonomous driving is located at the technology park of Andalucía.

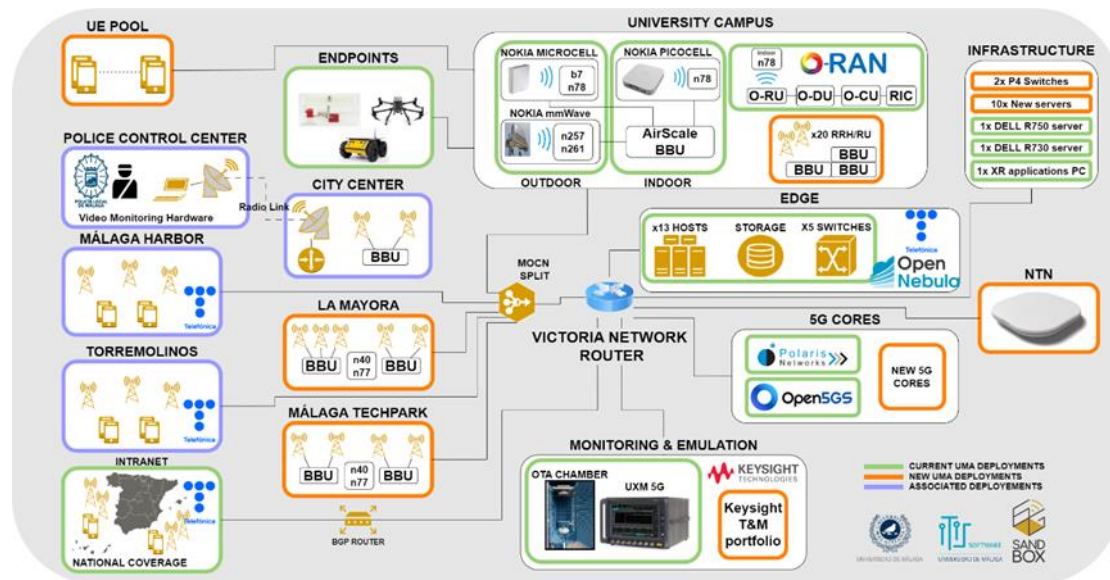


Figure 20: Victoria Network (Malaga's testbed).

Specifically, Victoria networks (as shown in Figure 20) support the following experimentation capabilities and equipment:

- Full automation of experimentation and testing of indoor deployment with local and remote access (mainly based on Open5Genesis suite and commercial testing tools).
- First-class emulators for 4G and 5G (including mmWave support up to 39GHz).
- Remote heads and multiple-frequency bands for cellular connectivity from NOKIA: 2.6 GHz for 4G LTE micro and pico cells, 3.5 GHz for 5G NR micro and pico cells, 26 GHz and 28 GHz for 5G NR (Release 16).
- O-RAN solution from Accelleran supporting control/user plane separation.
- Software for core network of 4G (EPC) and 5G (NSA and SA) from Polaris (Motorola Solutions) (Release 16), Open5GS.
- Movistar Intranet allows secure access to the UMA corporate network. Movistar Intranet allows access from the Movistar public network (Movistar SIM) to the private 5G network hosted at the UMA. The Movistar Intranet solution has the following components:

- 5G access network: TME's Mobile Telephony network is based on the Smart Network concept, a platform built on the basis of an interconnection of nodes where computer applications, switching centers and real-time database systems reside.
- Mobile ISP Mobile Network Core (MISP): Radius provided by UMA that handles the authentication of users accessing the network, assigning them an IP address from the client's private addressing plan.
- Data network: Telefónica's transport network that carries traffic from the public network to the company's headquarters, in this case the UMA. Fibre optics between the power station closest to the headquarters of the UMA.
- NEMO handy drive test tool from Keysight.
- Measurement tools for mobile devices based on iPerf and Ping utilities.
- Equipment to record SIM cards.
- Commercial mobile devices (One plus 9, One plus 11, Pixel 5, Asus 5G mmWave, Netgear routers, Askey routers).
- K8s.
- OpenNebula.
- OpenTAP (for automation).

A future extension of the testbed is the Integration of fixed/RAN and NTN (Non-terrestrial Networks) with EDGE/MEC, and use of OneWeb satellite mobile backhaul.

13.2.3 TNOR Testbed

Telenor's Large-scale Testbed in Norway provides an end-to-end facility for 5G (and beyond) experimentation in a *near-commercial* setting. It includes a central site in Fornebu as well as several edge and RAN sites across the country, which are interconnected by Telenor Norway's commercial transport network with high bandwidth VPNs. The key capabilities supported are as follows: (i) E2E network slicing with the option of *customised* network slice, (ii) E2E network orchestration and service orchestration, (iii) cloud-native infrastructure, (iv) next generation RANs, (v) 5G standalone (SA) multivendor core, (vi) next generation Firewall as a service. Figure 21 shows the Telenor LST functional architecture. As a supplement, the Mobile Data Access (MDA) Go service is also available in the facility, which allows any mobile device connected to Telenor commercial 5G network (Non-Standalone) to access the computing platform through a private Access Point Name (APN). This mitigates limitations on LST's coverage, capacity, and availability of SA-compliant devices.

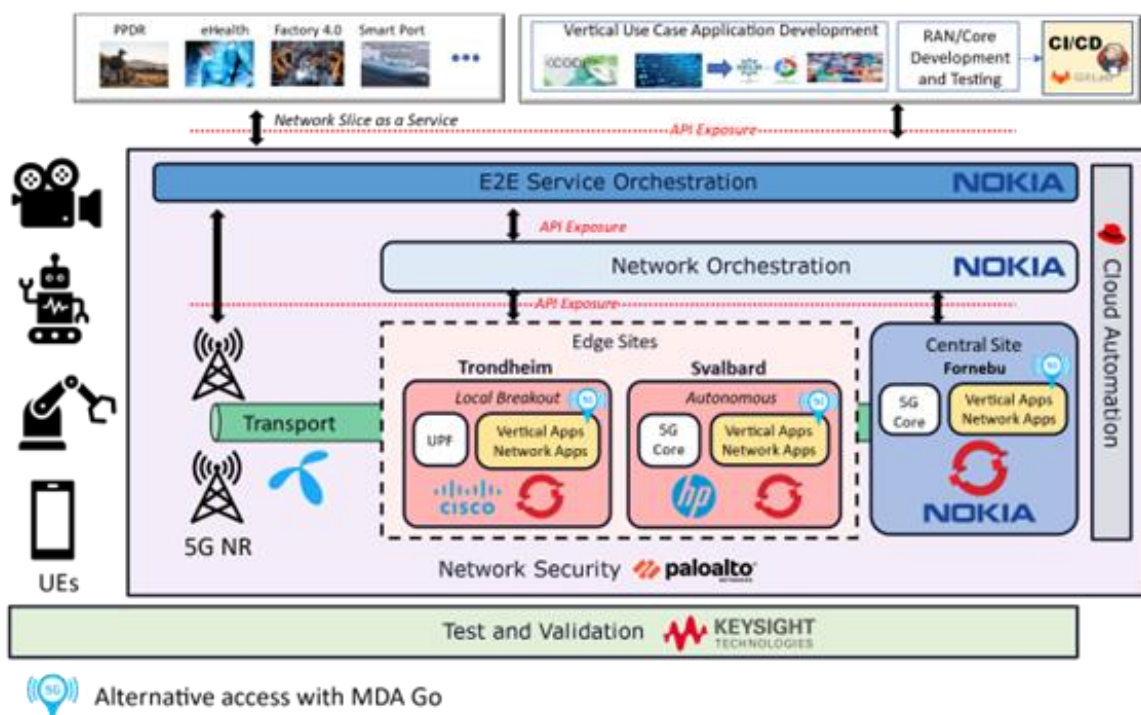


Figure 21: Telenor LST architecture.

The key RAN sites that can support different vertical experiments and basic configurations are provided below, in Table 54.

Table 54: Basic radio site configurations.

Site	Scope	Operational	Frequency NR	BW	Mode
Fornebu, Oslo (TBC)	Outdoor	Yes	3.3 – 3.4 GHz	100 MHz	SA
Trondheim - NTNU	Indoor	Yes	3.61-3.7 GHz	90 MHz	SA
		No	26 GHz	TBC	SA
	Outdoor	No	26 GHz	TBC	SA
Svalbard	Outdoor	Yes	3.7 – 3.8 GHz	100 MHz	SA

The virtualisation platform is based on Red Hat OpenShift Container Platform, and Single Node OpenShift (SNO) is used for small form factor edge sites. Private registries based on Red Hat Quay are used in the platform, which could be integrated with GitHub, GitLab and more for CI/CD.

The facility has a full-stack orchestration, supported by RedHat (infrastructure orchestration) and Nokia (network service orchestration). RedHat's Ansible Automation Platform (AAP) is used to manage the compute infrastructure, but also applicable to workload deployments. Nokia's NFVO – Nokia Cloud Operations Manager (NCOM) – is used for managing the 5G SA core components across all the sites. As for the E2E service orchestrator, Nokia's Orchestration Center (NORC) is used, which will be the main customer-facing component of the platform, offering Network Slice as a service and exposing interfaces such as the TM Forum OpenAPIs listed below in Table 55, together with the Unified Inventory.

Table 55: Supported TM Forum APIs.

Component	API	Purpose
NORC	TMF633 Service Catalog API	It allows the management of the Service Catalogue Elements lifecycles, and information on the service catalogue elements for the ordering process
	TMF641 Service Ordering Management API	The service Order can be created based on service that is defined in a catalogue. Service Order Operations: creation, deletion, change
	TMF645 Service qualification API	Provides service availability at Customer location
Unified Inventory	TMF638 Service inventory API	Provides a consistent/standardised mechanism to query and manipulate the Service inventory.
	TMF639 Resource inventory API	Provides a consistent/standardised mechanism to query and manipulate the Resource inventory.

To provide the zero-trust security, PaloAlto provides next generation Firewall as a service with features such as data leakage protection, application and protocol decoding, encrypted traffic inspection and signalling storm mitigation. As regards testing and validation, KeySight Technologies provides a Testing as a Service framework (details TBC), which includes a variety of testing tools and allow creating custom test campaigns.

14 Internal design of the FIDAL components

14.1 MAESTRO

14.1.1 Internal Architecture, Technologies, and baseline Assets

Figure 22 depicts a high-level functional architecture of Maestro that will be used as a baseline platform for FIDAL. At the northbound API, Maestro expects service providers to package their services in one or more containers forming a service graph. Once a containerised service is available, Maestro offers a UI (and a northbound API) that allow service providers to onboard the containerized service in an intuitive manner (step 1 in Figure 22). In step 2, a complete service is declared in Maestro's language and service providers can order an instance of this service. This requires Maestro to create a service-level slice (step 3 in Figure 22), formulate a slice intent message towards a specific OSS (step 4 in Figure 22), and dispatch this slice intent message to the underlying OSS (step 5 in Figure 22).

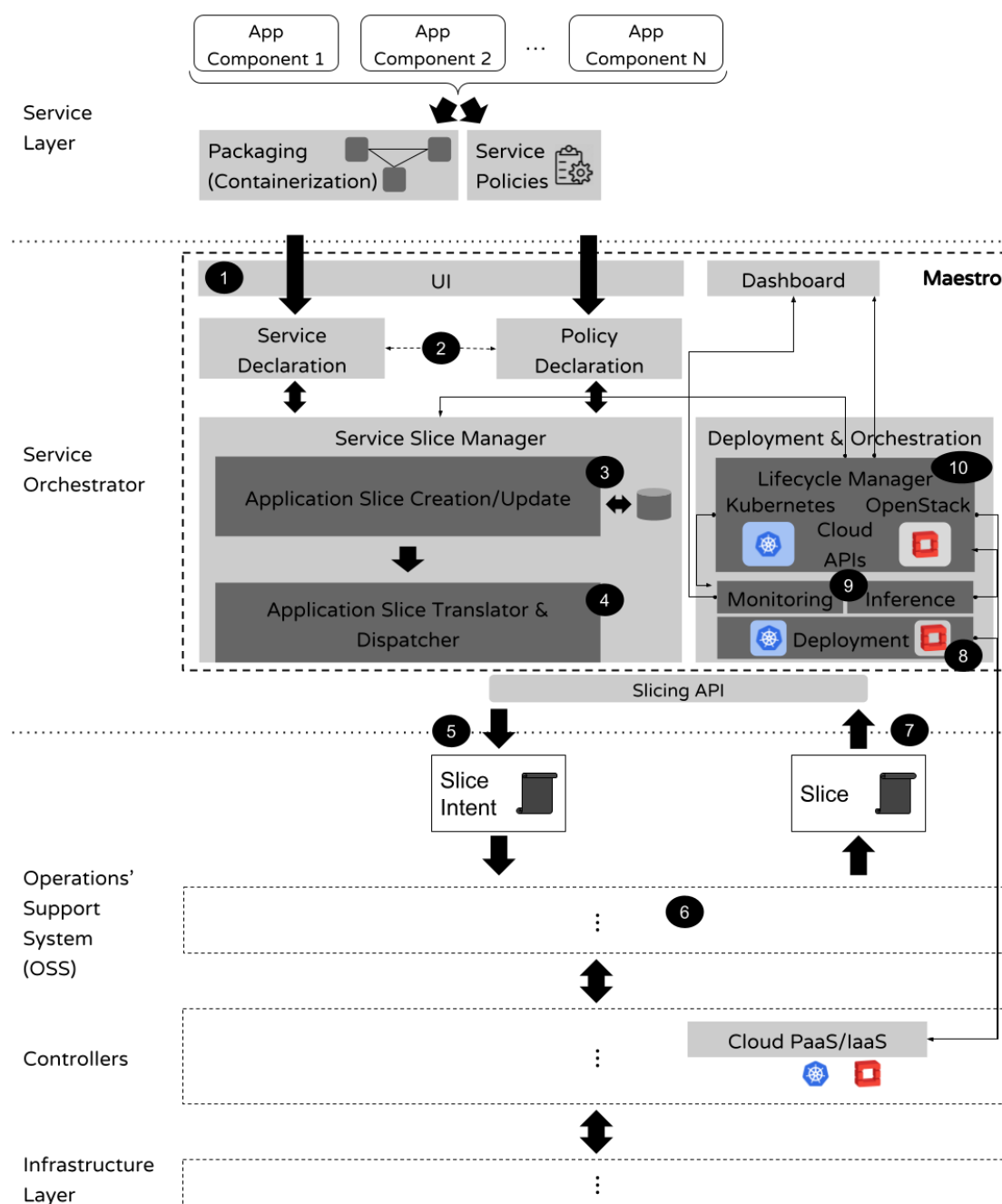


Figure 22: Maestro's high-level architecture.

Note that steps 3-5 are necessary for a service deployment as Maestro is a service-level orchestrator, thus does not have a direct view of the underlying infrastructure (only infrastructure-level do have such view). For this reason, Maestro requests a certain amount of compute and network resources (i.e., a slice) to be allocated by an OSS, on top of which then Maestro performs service deployment. When the underlying OSS allocates the requested slice (step 6 in Figure 22), the slice is returned back to Maestro (step 7 in Figure 22) and service deployment begins. In this step Maestro takes control of the allocated slice by connecting to the designated endpoints of the virtual infrastructure to initiate service deployment (step 8 in Figure 22). Maestro allows service providers to deploy their services atop both Infrastructure as a Service (IaaS) platforms, such as OpenStack and Platform as a Service (PaaS) platforms, such as Kubernetes. Maestro's deployment engine spawns the appropriate containers in the case of a Kubernetes or Virtual Machines (VMs) in the case of OpenStack and requests the monitoring module to deploy its monitoring routines (step 9 in Figure 22). Finally, during service runtime, Maestro invokes a dedicated LCM component for managing the lifecycle of deployed service instances, as shown in step 10 in Figure 22.

14.1.2 Functional Requirements

Table 56 below, depicts key functional requirements of Maestro for a successful integration with the rest of FIDAL's ecosystem.

Table 56: Maestro's functional requirements.

FR-ID	FR-Description	Related Module(s)/ Component(s)
FR1	Access to the FIDAL services repository through a stable API	FIDAL services repository
FR2	Offer FIDAL services to trial users and open call users through TM Forum's service catalog API (northbound/user facing API)	Users
FR3	Support TM Forum's service order and inventory APIs in collaboration with OpenSlice (southbound API)	OpenSlice
FR4	Manage cloud applications through a stable API on each testbed	Testbeds
FR5	Manage telemetry agents per application component	Testbeds
FR6	Consume telemetry in Prometheus format	Testbeds

14.1.3 External APIs

Maestro requires several external interfaces that enable communication with adjacent components for service orchestration, data collection, and consumption of reusable artefacts. These interfaces, shown in Table 56, include:

- the FIDAL services repository through interface i7;
- the northbound API towards FIDAL trial users and open call users through interface i9;
- the southbound API towards OpenSlice through interface i1;
- the testbeds' service and telemetry exposure APIs through interfaces i2 and i3; and
- the monitoring analytics framework and AlaaS using i4.

14.1.4 Maestro Extensions throughout FIDAL

Maestro will be upgraded with additional northbound and southbound APIs to facilitate the integration with OpenSlice and other FIDAL components. Specifically, Maestro today supports a custom service catalogue API (user facing NBI) and a custom slicing API (southbound API towards OSS). In the context of FIDAL, both of these APIs will be enriched. At the NBI, Maestro will implement a new TMF compliant service catalogue API (through interface i9), which will allow FIDAL users to create/read/update/delete FIDAL services, but also exchange services with OpenSlice's service catalogue, which also supports TMF. At the SBI, Maestro will implement a new TMF-compliant service order API (through interface i1) that will allow FIDAL users to associate services with the underlying 5G and compute resources (offered by OpenSlice as a service to Maestro). Other extensions will include: (i) support for service-level KPI monitoring and analytics (through interfaces i3 and i4), (ii) the management of automation through AlaaS, and (iii) the integration with the FIDAL services repository through interface i7.

14.2 OpenSlice

OpenSlice is an open-source operations support system designed to provide support for VNF/NSD onboarding and management. The platform supports TMFORUM OpenAPIs related to Service Catalog Management, Ordering, Resource, and more. It enables NFV developers to onboard and manage VNF and network service artifacts, while allowing vertical customers to browse available service specifications.

14.2.1 Internal Architecture, Technologies, and baseline Assets

Openslice (see Figure 23) will serve as the cross-domain slice manager in FIDAL, providing a repository of FIDAL Service Specifications that can be ordered by the Slice Intent handler of Maestro. Additionally, the Service and resources inventory will offer run-time information about the underlying entities created over the cross-domain end-to-end network fabric. The OpenSlice service orchestrator will be responsible for provisioning and delivering the network slice to the Maestro application service, as well as managing the slice's entire lifecycle. OpenSlice, besides APIs, offers the following user-friendly portals:

- The Services portal, which provides access to services.
- The NFV portal, which allows users to self-manage NFV artifacts and onboard them to a target MANO/NFV Orchestrator. Third-party applications can also access OpenSlice through TMForum Open APIs.
- The testing portal which allows to define testing services (this requires an external testing service).
- The resources portal, to manage any resources that are related to services.
- The products portal, to expose services as products.

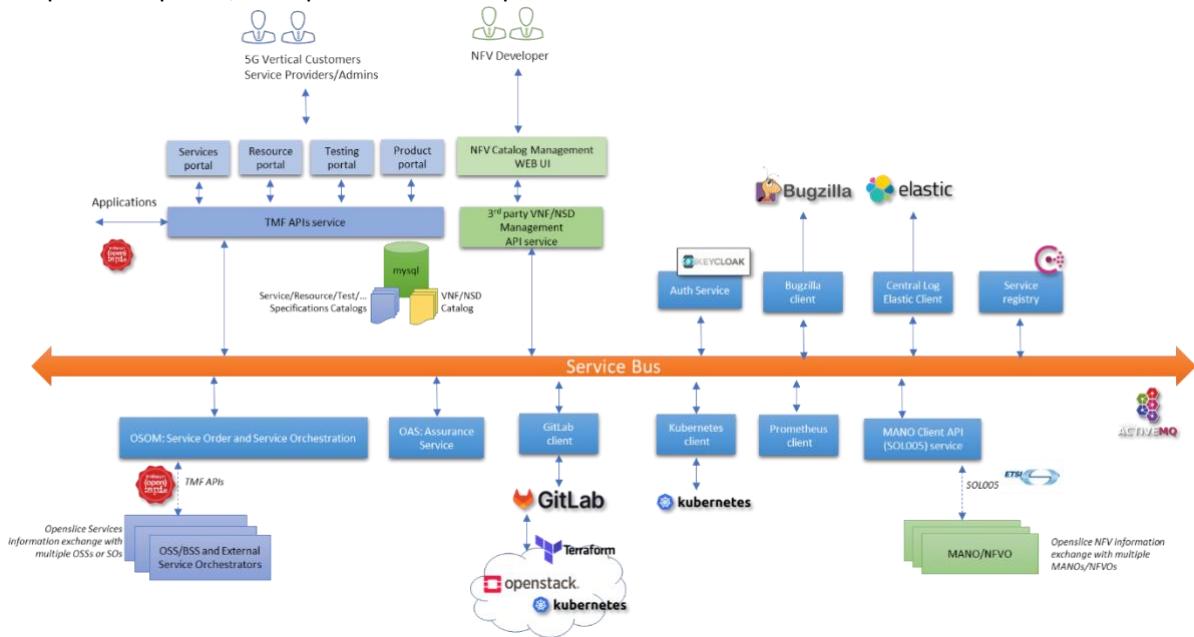


Figure 23: OpenSlice Architecture.

14.2.2 Functional Requirements

Table 57 captures the functional requirements of OpenSlice.

Table 57: OpenSlice's functional requirements.

OpenSlice		
FR-ID	FR-Description	Related Module(s)/ Component(s)
FR7	Use TM Forum API as northbound interface	Maestro
FR8	Consume telemetry in Prometheus format	Testbeds
FR9	Have access through a stable API to manage cloud resources for each testbed	Testbeds

FR10	Have access through a stable API to manage transport resources (switched, routers, load balancers, etc)	Testbeds
-------------	---	----------

14.2.3 External APIs

OpenSlice relies on various external interfaces to facilitate seamless communication with its adjacent components. These interfaces serve multiple purposes, including service and slice orchestration, data collection, and consumption of reusable artifacts. The key interfaces involved in this process are as follows:

1. Interface i1: OpenSlice communicates with the Maestro component through this interface. It enables the coordination and management of services and slices within the architecture.
2. Interfaces i2 and i3: OpenSlice establishes connections with the testbeds through these interfaces. They facilitate the exchange of data and control information necessary for testing and validation activities.
3. Interface i4: OpenSlice utilizes this interface to interact with monitoring analytics. It enables the collection and analysis of relevant data for performance monitoring and optimisation purposes.
4. Interface i6: OpenSlice connects with the repository via this interface. It enables the retrieval and utilisation of reusable artifacts, such as configurations, images, models, and templates.

The utilisation of these external interfaces enhances the functionality and interoperability of OpenSlice within the broader system architecture.

14.2.4 OpenSlice extensions throughout FIDAL

As part of an upcoming upgrade, OpenSlice is being enhanced to support coexistence and interoperability with MAESTRO through its northbound interface. This upgrade will enable OpenSlice to play a distinct role within the overall architecture, focusing on automated orchestration and management of the end-to-end infrastructure.

The upgraded OpenSlice will introduce several additional extensions to enhance its capabilities:

1. Interoperability with MAESTRO: OpenSlice will establish compatibility with MAESTRO, allowing seamless integration and communication through the northbound interface.
2. KPI Monitoring: OpenSlice will incorporate support for Key Performance Indicator (KPI) monitoring. This feature will enable the tracking and analysis of essential metrics to ensure optimal performance of the system.
3. Repository Service: OpenSlice will introduce a repository service to facilitate the reusability of resources and artifacts. This repository will serve as a centralized hub for storing and accessing configurations, models, templates, and other reusable components.
4. Automation Management through AlaaS: OpenSlice will integrate capabilities for managing automation through AI-as-a-Service (AlaaS). This integration will enable efficient and intelligent automation of tasks and processes within the architecture.

These upgrades will empower OpenSlice to function as a robust and versatile component, contributing to the seamless orchestration and management of the overall infrastructure.

14.3 AlaaS Component

AlaaS is a component for executing Deep Learning/Machine Learning models and managing their resulting data. Its purpose is being the heart of model serving, by providing out-of-the-box support for popular DL/ML frameworks and unparalleled performance. AlaaS will support specific methods for data processing (based on Pandas facilities) and algorithmic workflow composition, including train/test dataset splitting, quick Search cross-validation for parameter tuning, fitting methods, predictive modelling and quality metrics (ROC, Confusion Matrices, R^2 , RMSE, etc). All these specific methods will be based on Python libraries such as ScikitLearn, PyTorch, Tensorflow (libtensorflow), TensorFlow Lite, Keras and more specified upon specific needs backends. This extremely important since the serialisation mechanism of one version might not match with another. For making sure that the AI models will work with the FIDAL internal APIs, we will adopt open data exchange standards (CSV, JSON, etc.) and ensure compatibility at the early stage of deployment. For validation purposes and documentation, a set of Jupyter Notebooks will be provided as demonstrators with specific example use cases oriented to data processing, exploratory analysis of variables and predictive modelling. Generated datasets for training will be also made available through the API methods.

14.3.1 Internal Architecture, Technologies, and Baseline Assets

The data analysis pipeline required for the data training includes a set of steps. In the beginning of the pipeline some data engineering operations, including data cleaning, alignment and transformation will be performed. As part of data preparation, indexing, joins, enrichment, feature engineering, selection and merging with underlying data will be executed. Last, the curated data will be fed to the AI model for building and training. As part of the model serving as depicted in the figure below (Figure 24), any client application or process needs to trigger the AI Model Server with a key to reference data model to get the corresponding result. The AI model result according to the supported task (e.g., regression, classification or other) will return the results by means of scalar or vectorised data. If the resulting data need to be further structured, a JSON or a Pub/Sub interface will be delivered during the integration phase.

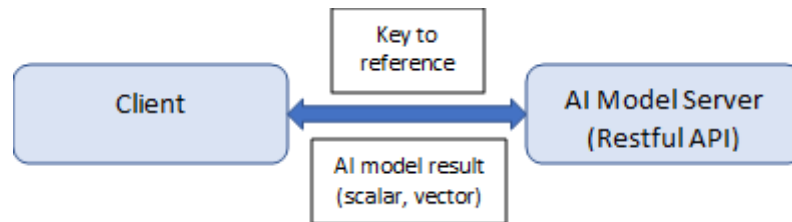


Figure 24: Data Analysis Pipeline.

14.3.2 Functional Requirements

Table 58: Functional Requirements of AlaaS Component.

AlaaS Component		
FR-ID	FR-Description	Related Module(s)/ Component(s)
FR11	Harvest telemetry data from Elastic to train regression models	Maestro
FR12	Harvest telemetry data from Elastic to train classification models	Maestro
FR13	Harvest telemetry data from Prometheus to train regression models	Testbeds
FR14	Harvest telemetry data from Prometheus to train classification models	Testbeds

14.3.3 External APIs

The AlaaS Component requires a number of external interfaces that enable to harvest data for analysis to train and keep the AI models updated. These include i4 which harvests data coming from monitoring analytics regarding Maestro and OpenSlice, and i8 which serves the inference result of the AI models.

14.4 Monitoring Analytics

The monitor analytics platform is part of the experimentation framework of FIDAL responsible for collecting the data from the respective data sources, calculating the necessary KPIs for each case, persisting the data into the internal database and finally providing the means to the end user to visualise and export the data.

14.4.1 Internal Architecture, Technologies, and Baseline Assets

The platform consists of five microservices aiming to segregate the functionality for both development purposes and availability. The five submodules are:

- the **data collector** for collecting, harmonizing and persisting the data from all available data-sources;
- the **KPI modeler** responsible for calculating the necessary KPIs;

- the **database** for persisting the KPIs;
- the **visualization portal** for providing the visualization dashboards to the end users;
- the **internal REST API** for providing the necessary functionality to the visualization portal.

The above submodules and the internal architecture comprising the monitoring analytics platform can be seen in Figure 25.

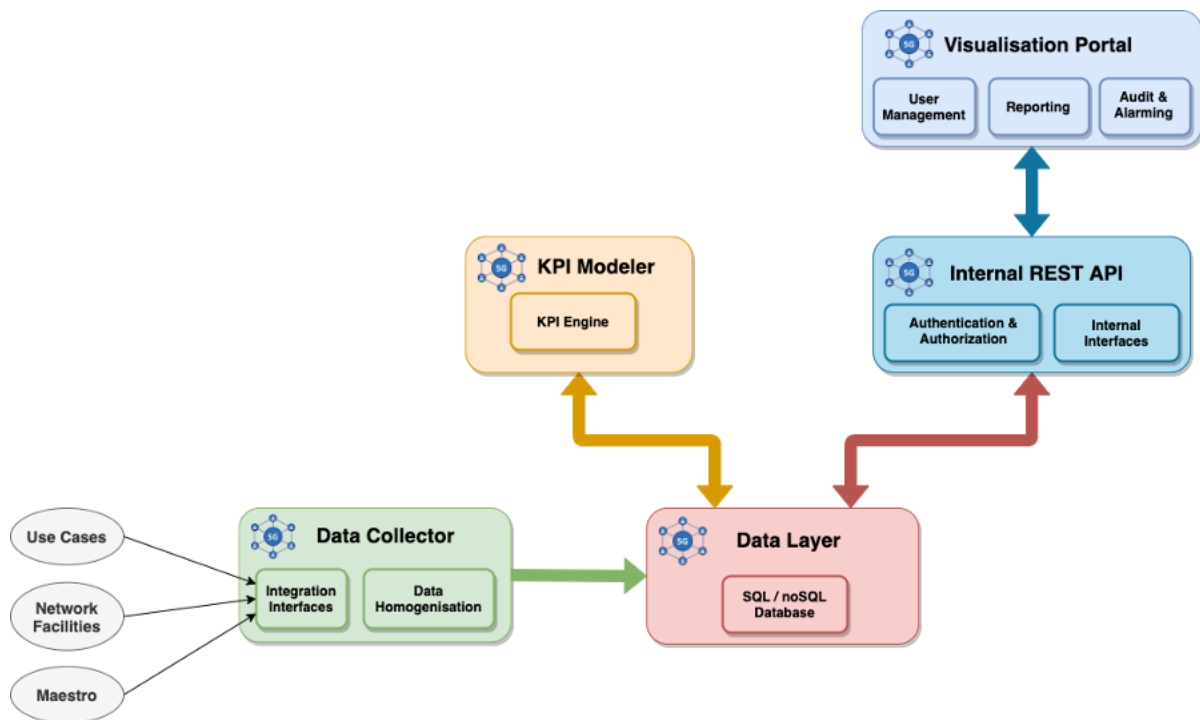


Figure 25: Monitoring Analytics platform internal architecture.

a) **Data Collector**

The data collector module is responsible for:

- Collecting data from all available data sources including the use cases, the underlying facilities and the vertical application orchestrator (MAESTRO);
- Homogenising the incoming data into one common data structure that will enable the postprocessing;
- Persisting the data into the internal database.

The data ingestion flow will include a REST API that will be exposed to be consumed by the remote parties that can support it and the open calls applications. For 3rd parties - within the project - that prefer other integration means, the data collector will implement other integration protocols to support the interconnection. The data collector will be developed in Java (version 17) and will be based on the Spring Boot framework. It will be dockerised and the container will be orchestrated by a Kubernetes cluster.

b) **Data Layer**

The data layer includes the internal database of the monitor analytics module. It stores the incoming raw data, the harmonised data along with the resulting KPIs. All other metadata of the platform such as the users, the login audit etc. are also stored here.

The database used is pending to be decided. The options are either PostgreSQL or MongoDB depending on whether an SQL or non-SQL based database is preferred.

c) KPI Modeler

The KPI modeler is responsible for calculating the KPIs of each test case execution. It will utilise the raw data ingested and based on the requirements of each case will produce the KPIs required. The KPI modeler will be developed in Java (version 17) and will be based on the Spring Boot framework. It will be dockerised and the container will be orchestrated by a Kubernetes cluster.

d) Internal REST API

The internal REST API is the submodule responsible for providing access from the Visualisation portal to the data layer. It is a set of HTTP REST interfaces that provide the necessary data to the portal while also providing the means to authenticate and authorise the user making the request and authorise. The internal REST API will be developed in Java (version 17) and will be based on the Spring Boot framework. It will be dockerised and the container will be orchestrated by a Kubernetes cluster.

e) Visualisation Portal

The visualisation portal utilizes the internal REST API to visualize the KPIs of a test case execution through intuitive dashboards. Data is available in graphical and tabular data along with export functionality. Other functionality is also offered for privileged users such as user management and access control. The portal will be developed with the JavaScript/TypeScript language utilizing the Angular framework. UI components from PrimeNG (an open-source theme) along with some custom UI components will be used to satisfy the visualization requirements of the platform. It will be dockerised and the container will be orchestrated by a Kubernetes cluster.

14.4.2 Functional Requirements

Table 59: Functional Requirement of Monitoring Analytics.

Monitoring Analytics		
FR-ID	FR-Description	Related Module(s)/ Component(s)
FR15	The Data Collector will offer an integration interface in order to collect data from various sources	Testbed Maestro Openslice
FR16	The Data Collector will homogenise data into a common data structure	N/A
FR17	The Data Collector will persist the homogenised data to the Data Layer	N/A
FR18	The Data Modeller will calculate the respective KPIs and persist the results to the Data Layer	N/A
FR19	The Visualisation Portal will allow only authenticated users to use it	Users
FR20	The Visualisation Portal will present the KPIs in tabular and graphical format	Users
FR21	The Monitor Analytics platform will propagate the calculated KPIs to the FIDAL Services Repository	FIDAL Services Repository

14.4.3 External APIs

The monitoring analytics platform will need to ingest data from various data sources. For this purpose, an abstract REST API interface will be designed and implemented that will be exposed by the data collector to handle incoming data. This will be available for all internal project UCs but also for the open calls. Specifically for the internal UCs and the underlying 5G testbeds, in case integration with the aforementioned REST API is not possible for any reason, additional APIs may be agreed and implemented to assist on the component's onboarding to the analytics platform. Additionally, another REST API will be provided for exporting the data outside the data collector for 3rd party usage.

14.5 FIDAL repository services

The FIDAL Services Repository is responsible for the management and exposure of artefacts from the FIDAL framework as a service. Such artefacts may include datasets (e.g., KPI measurements, trace files, etc.) from experimentation, Network Applications container images, training sets and pre-trained models from the AlaaS system. FIDAL Repository Services aims to simplify the exposure of such artefacts both within the FIDAL community, and to the wider SNS and

research communities in the form of open data. To this end, a set of Backend Services for File Storage, Search, and Repository Management are deployed and integrated at ISI servers, alongside a custom Portal service acting as the Frontend which provides access to FIDAL artefacts. The Backend Services are integrated with the respective FIDAL framework components that via CRUD APIs.

14.5.1 Internal Architecture, Technologies, and Baseline Assets

The FIDAL Repository Services is responsible for “bookkeeping”, CRUD operations and search of project assets. Figure 26 shows the internal architecture of the Frontend and Backend services and how they are interconnected with private deployments of NextCloud and the JFROG Artifactory services. The former is responsible for handling of multiple categories of artefacts, while the latter is a dedicated registry server that stores and distributes container images for Network Apps.

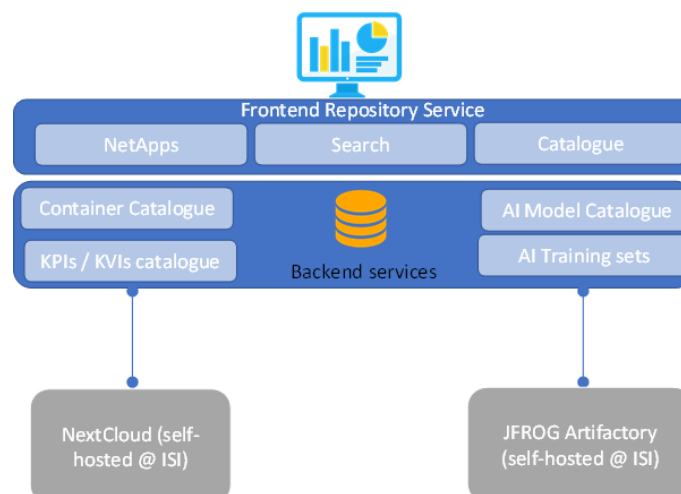


Figure 26: FIDAL Repository Services internal design.

14.5.2 Functional Requirements

The functional requirements of FIDAL Repository are presented below in Table 60.

Table 60: FIDAL Repository functional requirements.

FIDAL Repository Services		
FR-ID	FR-Description	Related Module(s)/ Component(s)
FR22	The system should provide File Storage for project assets and artefacts	NextCloud
FR23	Web based Frontend for Public and Private access	Frontend service
FR24	Multiple categories of file types and artefacts (e.g., Docker Images)	NextCloud, JFROG Artifactory
FR25	CRUD APIs towards FIDAL Framework components	Backend Service
FR26	Search and Catalogue functionalities	Backend Service

14.5.3 External APIs

The FIDAL Repository Services will offer APIs towards all FIDAL framework components, e.g., allowing the Monitoring and Analytics module to store experimentation files as a service via the i4 CRUD API. Moreover, the i5 API is offered towards the MAESTRO, supporting the capability to store container images for Network Apps.

15 Methodology for the vertical use case trial process

This section outlines the specific guidelines and methodologies for establishing experimentation platforms prior to conducting actual trials. It is crucial to establish a set of common guidelines and a robust methodology for the trial process of use cases to ensure smooth onboarding and execution. The underlying concept adopts the Network Slice as a Service (NSaaS)³⁸ delivery model, which involves provisioning customised network slices to verticals upon request. This allocates a network slice to the experimenters for use for testing, monitoring, and assessing Key Performance Indicators (KPIs) under various network conditions and use case scenarios. During this process, UE devices need to be allocated to experimenters, a proper scheduling of experiments need to be negotiated with the testbeds and FIDAL orchestrators will provision resources to the respective FIDAL facilities in order to provision the requested services. The proposed FIDAL onboarding process provides the necessary flexibility for experimentation, while any lessons learned during the trials will be reflected back to this process.

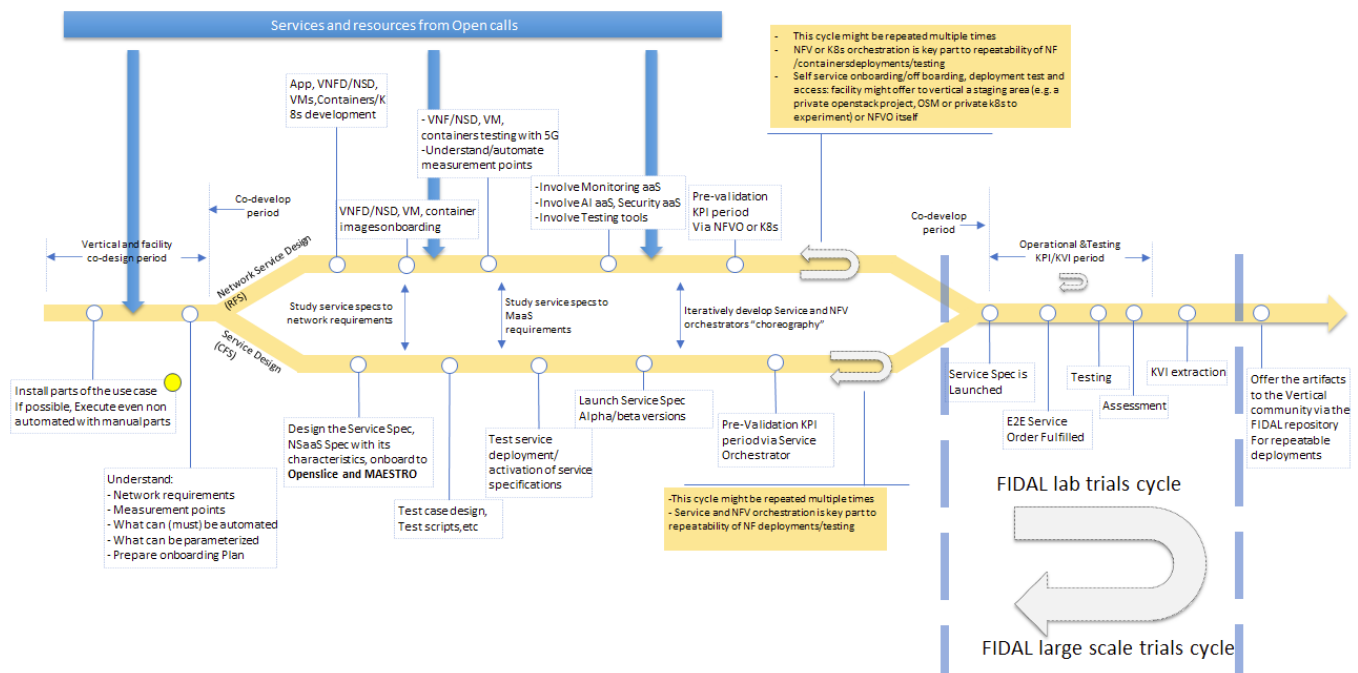


Figure 27: Onboarding lab testing and trials methodology.

The FIDAL methodology (see Figure 27) consists of three distinct periods:

1. Vertical and facility design period: During this phase, stakeholders such as vertical customers, facility owners, and CFS/RFS developers collaborate to understand the specifics of the verticals such as the requirements and automation needs and determine how to fulfil those effectively.
2. Development period: The iterative co-development period involves joint efforts between the vertical customer and the facility providers to develop the final service that will be ordered. This includes the development of Virtual Network Functions (VNFs), test scripts, and monitoring services. Integration of Testing as a Service (TaaS) and Monitoring as a Service (MaaS) can be carried out during the preparation of VNFs and the development of service templates.
3. Testing period: This phase allows the vertical customer to place repeatable and scheduled service orders based on the developed service blueprint through the portal. They can conduct KPI testing, monitoring, and assess activities during this period.

The final developed service specification can be uploaded and instantiated from a service catalogue, resources are reserved, orchestrated, and repeated for testbed and large-scale trials. All artefacts are stored at the FIDAL repository.

³⁸ 3GPP TS 28.530

16 Security requirements, methodology, processes definition and guidelines

The section of this document concerns the security factors of the FIDAL project. In order to introduce the security context, the following sections take copy from the relevant parts of the FIDAL Grant Agreement Description of Action for reference as well as establish the regulatory framework that guides FIDAL's security practices.

16.1 Requirements from the DoA

Innovation Area 5: Innovative Security Frameworks

Current SoTA & Challenges: The threat of sophisticated cyber-attacks looms large on networks. With the inflating possible attack surface of devices, software, AI, and network components, the menace it poses is potent and dynamic. 5G evolve & 6G networks will be designed to provide trusted services on a zero-trust infrastructure and protect against such larger scale traditional threats as well as new threats like jamming of mission critical private networks. Privacy issues will also need to be taken into cognizance when new mixed-reality worlds combining digital representations of real and virtual objects are created. What we need is a comprehensive set of security technology enablers for the Beyond 5G era, enhanced and supported by AI/ML and new principles of cyber-resilience. It is no surprise that trustworthiness has been identified as a key value objective and indicator for 6G by the European Union 6G flagship project Hexa-X²⁴.

Ambition: FIDAL's ambition is to provide a structured security framework focusing on Evolved 5G and 6G era ecosystems incorporating architectures, processes, technologies, enablers, vendors, service providers and subscribers. Within FIDAL's security framework, AI/ML will be used pervasively across 6G security architecture, process and technology domains. FIDAL's security methodology will be seek, and accommodate, new requirements as they arise in the future as well. Technologies as yet unknown may also call for FIDAL to enhance this initial set of cyber-resilience technology enablers. Our ambition is to define, apply, demonstrate, promote to the standard bodies and provide to the community (including 6G-IA SNS JU Phase II projects) a security framework targeting Evolve 5G and 6G ecosystems.

1.1.4 R&I maturity

Several research and innovation activities exhibit useful complementarities with the FIDAL project. The participation of common partners in these initiatives ensures good alignment as well as smooth collaboration and exchange of know-how, and the further development / enhancements of assets to increased TRL.

In FIDAL's 5G evolution and 6G security vision, we cluster security technology enablers into domains of cyber-resilience, privacy and trust, and their respective intersection. Our approach emphasizes the need to extend cyber-resilience technologies by privacy-preserving technologies and on top of that, trust-creating technologies and processes in order to achieve the ultimate goal of trustworthy 6G networks. We consider resilience against all kinds of cyber-attacks as the core element and indispensable foundation — a network that lacks these attributes of cyber-resilience will not be able to protect privacy and enable trust. While cyber resilience protects privacy against external attacks, end users may in addition want to reduce the amount of sensitive information that is revealed internally, i.e., to the multiple stakeholders involved in providing the communication services. Enabling technologies and processes are needed beyond those in the area of cyber resilience. FIDAL's security framework will aim at addressing the complete 5G evolution and 6G security threat landscape that will govern all project WPs including the Open Calls (WP5).

Objective 5 of the DoA is to implement an end-to-end security framework for project operations including AlaaS. The complexity of the ecosystem and use cases require security methods that include:

- A **live and ongoing library** of security controls and audits;
- An **action plan** (including evidence thereof) to respond to security issues;
- Creating and delivering **security awareness trainings** for different FIDAL stakeholder profiles.

Additionally, security in FIDAL will support building:

- **Business value**, particularly around solving existing and emergent problems;
- **Trust**, in ways that support measuring if and how the security framework supports trustworthiness among stakeholders;
- **Responsibility**, particularly in ways that engage **accountability, control, and impact** within the open ecosystem.

FIDAL will define, apply, demonstrate, promote to standard bodies, and provide to the community a comprehensive set of technological and organisational security enablers that are enhanced and supported by AI and new principles of cyber-resilience. These aim at addressing the complete 5G evolution and 6G security threat landscape within the project, including trials and open calls. FIDAL's approach emphasises the need to extend cyber-resilience technologies by privacy-preserving, trust-creating and resilience-building technologies and processes (e.g., from guarding against external attacks to reducing the amount of sensitive information that is revealed internally). Thus, this security framework must include architectures, processes, technologies, vendors, service providers, and subscribers.

The security framework will consist of:

FIDAL Security Management: a security committee, consisting of PSCE, NOVA, TNOR, TID, PNET, UOP, IQU, and UMAN, will manage the project security activities and act as a security consultant. The project will prioritise the continuous evaluation of security across the WPs and trials, via requirements, architectures, and methodologies.

5G evolution: critical to FIDAL security are AI/ML, zero-touch, multi-vendor environment and onboarding of open-source applications.

Experimentation: security-by-design will be prioritised as a key consideration during innovative and transformative work.

Open Calls and Third-Party Support: application programming interfaces must be secure and not share restricted credentials. In addition, service level agreements or contractual observations of third parties need to be drafted in order to engage secure, open collaboration.

Validation in large scale and open call trials: security-by-design must be communicated to trial and use case stakeholders in ways that are readily and easily understandable.

Societal Impact Analysis: working via co-design, input will be sought from a diverse expertise and skill set, serving to define and apply security as well as to illustrate security requirements and awareness of stakeholders.

Secure AI as a Service: Implicit within FIDAL's AlaaS provision, FIDAL will use a security software development life cycle approach, identifying security baseline KPIs and KVIs, providing a qualitative AI security scorecard that underpins value, data, and governance, and security audits (with appropriate mitigation measures). The project will provide advanced infrastructure, lowered costs and reduced need for development teams to have ML expertise. Models developed will not serve end-users directly but support those building solutions, combining top-down vertical sector requirements with bottom-up innovative technical capabilities and inclusive and collaborative human engagement (via views and experiences of NetApp developers). In particular, security will focus on data security, reliability, transparency, data governance, accessibility, and responsible oversight that mitigate the potential for AI to produce harmful unintended outcome, service discrimination, unsafe data handling, and compliance failures.

16.2 DoA FIDAL Security Declaration

All partners have agreed to a Security Declaration as to these points above, including:

- The required documents, information and results related to FIDAL will be duly protected and not lead to exposure of sensitive information in cybersecurity contexts (in particular, to entities not established in the Member States or controlled from third countries).
- The infrastructure deployed within FIDAL shall remain, during the action and one (1) calendar year after its completion, within the beneficiary/beneficiaries and shall not be subject to control or restrictions by entities not established in the Member States or controlled from third countries.

- The FIDAL Consortium will comply to Commission requests for security measures to be implemented in the project and/or to carry out a security scrutiny focusing on the exchange of project information, documents, and results considered as security-sensitive information among project partners. Due account will be taken of exceptional circumstances, and notably where needed equipment or services cannot be provided from entities established in the Member States or controlled from third countries.

Objective 5 of the DoA is to implement an end-to-end security framework for project operations including AlaaS. The complexity of the ecosystem and use cases require security methods that include:

- A **live and ongoing library** of security controls and audits;
- An **action plan** (including evidence thereof) to respond to security issues;
- Creating and delivering **security awareness trainings** for different FIDAL stakeholder profiles.

Additionally, security in FIDAL will support building:

- **Business value**, particularly around solving existing and emergent problems;
- **Trust**, in ways that support measuring if and how the security framework supports trustworthiness among stakeholders;
- **Responsibility**, particularly in ways that engage **accountability, control, and impact** within the open ecosystem.

FIDAL will define, apply, demonstrate, promote to standard bodies, and provide to the community a comprehensive set of technological and organisational security enablers that are enhanced and supported by AI and new principles of cyber-resilience. These aim at addressing the complete 5G evolution and 6G security threat landscape within the project, including trials and open calls. FIDAL's approach emphasises the need to extend cyber-resilience technologies by privacy-preserving, trust-creating and resilience-building technologies and processes (e.g., from guarding against external attacks to reducing the amount of sensitive information that is revealed internally). Thus, this security framework must include architectures, processes, technologies, vendors, service providers, and subscribers.

The security framework will consist of:

FIDAL Security Management: a security committee, consisting of PSCE, NOVA, TNOR, TID, PNET, UOP, IQU, and UMAN, will manage the project security activities and act as a security consultant. The project will prioritise the continuous evaluation of security across the WPs and trials, via requirements, architectures, and methodologies.

5G evolution: critical to FIDAL security are AI/ML, zero-touch, multi-vendor environment and onboarding of open-source applications.

Experimentation: security-by-design will be prioritised as a key consideration during innovative and transformative work.

Open Calls and Third-Party Support: application programming interfaces must be secure and not share restricted credentials. In addition, service level agreements or contractual observations of third parties need to be drafted in order to engage secure, open collaboration.

Validation in large scale and open call trials: security-by-design must be communicated to trial and use case stakeholders in ways that are readily and easily understandable.

Societal Impact Analysis: working via co-design, input will be sought from a diverse expertise and skill set, serving to define and apply security as well as to illustrate security requirements and awareness of stakeholders.

Secure AI as a Service: Implicit within FIDAL's AlaaS provision, FIDAL will use a security software development life cycle approach, identifying security baseline KPIs and KVs, providing a qualitative AI security scorecard that underpins value, data, and governance, and security audits (with appropriate mitigation measures). The project will provide advanced infrastructure, lowered costs and reduced need for development teams to have ML expertise. Models developed will

not serve end-users directly but support those building solutions, combining top-down vertical sector requirements with bottom-up innovative technical capabilities and inclusive and collaborative human engagement (via views and experiences of NetApp developers). In particular, security will focus on data security, reliability, transparency, data governance, accessibility, and responsible oversight that mitigate the potential for AI to produce harmful unintended outcome, service discrimination, unsafe data handling, and compliance failures.

16.3 DoA FIDAL Security Declaration

All partners have agreed to a Security Declaration as to these points above, including:

- The required documents, information and results related to FIDAL will be duly protected and not lead to exposure of sensitive information in cybersecurity contexts (in particular, to entities not established in the Member States or controlled from third countries).
- The infrastructure deployed within FIDAL shall remain, during the action and one (1) calendar year after its completion, within the beneficiary/beneficiaries and shall not be subject to control or restrictions by entities not established in the Member States or controlled from third countries.
- The FIDAL Consortium will comply to Commission requests for security measures to be implemented in the project and/or to carry out a security scrutiny focusing on the exchange of project information, documents, and results considered as security-sensitive information among project partners. Due account will be taken of exceptional circumstances, and notably where needed equipment or services cannot be provided from entities established in the Member States or controlled from third countries.

16.4 EU and National Regulatory and Standards Foundation

In addition to what is already written, there are four most relevant and recent European legislative instruments for which the project will follow as it designs and implements its security framework:

- Cyber Security Act 2019³⁹ (proposed to be updated in 2023) which mandates the EU Agency for Cyber Security (ENISA) for its role towards developing cyber security certification in addition to its advisory services.
- Critical Entities Resilience (CER) Directive 2022⁴⁰ and recommendation which aims to reduce vulnerabilities and strengthen resilience of critical entities. This includes resilience of infrastructure for telecommunications.
- Network and Information Security (NIS2) Directive 2022⁴¹ which imposes obligations on all critical infrastructure providers and digital service providers operating in the EU to implement appropriate technical and organizational measures to manage the risks posed to the security of their network and information systems.
- General Data Protection Regulation (GDPR) 2016⁴² with primary aim is to enhance individuals' control and rights over their personal data and to simplify the regulatory environment for international business.
- Artificial Intelligence Act (proposed 2021) 2023⁴³ with the primary aim to lay down rules to follow a risk-based approach and establish obligations for providers and users depending on the level of risk the AI can generate.

Nationally, each country is obliged by the NIS2 Directive to implement a Cyber Security Incident Response Team (CSIRT). ENISA holds the role of secretariat for the CSIRTs network⁴⁴. CSIRTs typically also provide national guidance on cyber security matters. Each partner shall make contact with their CSIRT to become aware of the guidance they provide, and in case any incident must be reported.

³⁹ Cyber Security Act: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>

⁴⁰ CER Directive: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj>

⁴¹ NIS2 Directive: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

⁴² GDPR Regulation: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504>

⁴³ Artificial Intelligence Act: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206>

⁴⁴ <https://csirtnetwork.eu>

In addition, security methodology in FIDAL will follow the main principals of EU Toolbox for 5G Security⁴⁵. In 2021, the European Commission published the EU Toolbox for 5G Security which provides a high-level view of security risk analysis and approaches to take for protection considering both technical and supply chain matters. This toolbox is primarily targeted towards Member State guidance to provide nationally for 5G deployments, building upon 5G trials such as those to be implemented in FIDAL. A progress report on the use of the toolbox has been released on 15th June 2023⁴⁶. The report includes **recommendations for Member States** to:

- Ensure they have **comprehensive and detailed information** from **mobile operators** about the 5G equipment currently deployed and about their plans for deploying or sourcing new equipment.
- In **assessing the risk profile of suppliers**, Member States should consider the objective criteria recommended in the EU Toolbox. In this context, it is evident that 5G suppliers exhibit **clear differences in their characteristics**, in particular as regards their likelihood of being influenced by specific third countries which have security laws and corporate governance that are a potential risk for the security of the Union. Furthermore, **designations made by other Member States** concerning high-risk suppliers should be taken into account, with a view to promote consistency and a high level of security across the Union.
- Based on the assessment of suppliers, **Member States should impose restrictions on high-risk suppliers without delay**, i.e., considering that a loss of time can increase vulnerability of networks in the Union and the Union's dependency on high-risk suppliers, especially for Member States with a high presence of potential high-risk suppliers.
- To effectively mitigate risks, Member States should ensure that the **restrictions cover critical and highly sensitive assets** identified in the EU Coordinated risk assessment, **including the Radio Access Network**.
- For types of equipment covered by the restrictions, operators **should not be allowed to install new equipment**. If transition periods are allowed for the removal of existing equipment, they shall be defined to ensure the **removal of equipment in place within the shortest possible timeframe**, taking into account the security risk of keeping equipment from high-risk suppliers in place, and should not be applied to allow the continued deployment of new equipment from high-risk suppliers.
- Implement **restrictions for Managed Service Providers (MSPs)**, and in case functions are outsourced to MSPs, impose enhanced security provisions around the access that MSPs are given.
- Further discuss the **applicability of measures related to diversification of suppliers**, and how to best ensure that any potential diversification does not result in new or increased security risks but contributes to security and resilience.
- **Enforce technical measures** and ensure a **strong level of supervision**. Particular attention should be given to certain measures, notably ensuring the application of baseline security requirements, raising security standards in suppliers' processes through robust procurement condition and ensuring secure 5G network management, operation and monitoring.

16.5 Driving Security Motivations

This section builds upon knowledge of the many dimensions of trust brought now by the 5G standards, and the different viewpoints considering the FIDAL testbeds, components and how the societal benefit is driven by Secure Key Values.

16.5.1 Trust and expertise viewpoint

An analysis of potential 5G Innovations⁴⁷ was produced in the early days of 5G research. This document raises concern surrounding the introduction of virtualisation into the mobile standards, and the increased degrees of freedom on the system both in terms of technical components due to virtualisation, and the increased dynamic of the diversified supply chain. We move from a small number of large trusted mobile telecoms vendors and operators to a broader supply chain of less trusted components, their developers, integrators and operators.

⁴⁵ <https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security>

⁴⁶ https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3309

⁴⁷ <https://www.slideshare.net/TechUK/5g-innovation-opportunities-a-discussion-paper>

Figure 28 illustrates the core nature of impact from a holistic security perspective. It maps the question of who trusts who in both the technical and information supply chains, as well as which components trust which. This latter view can be seen in a technical way, for example binding technical trust through exchange of crypto keys.

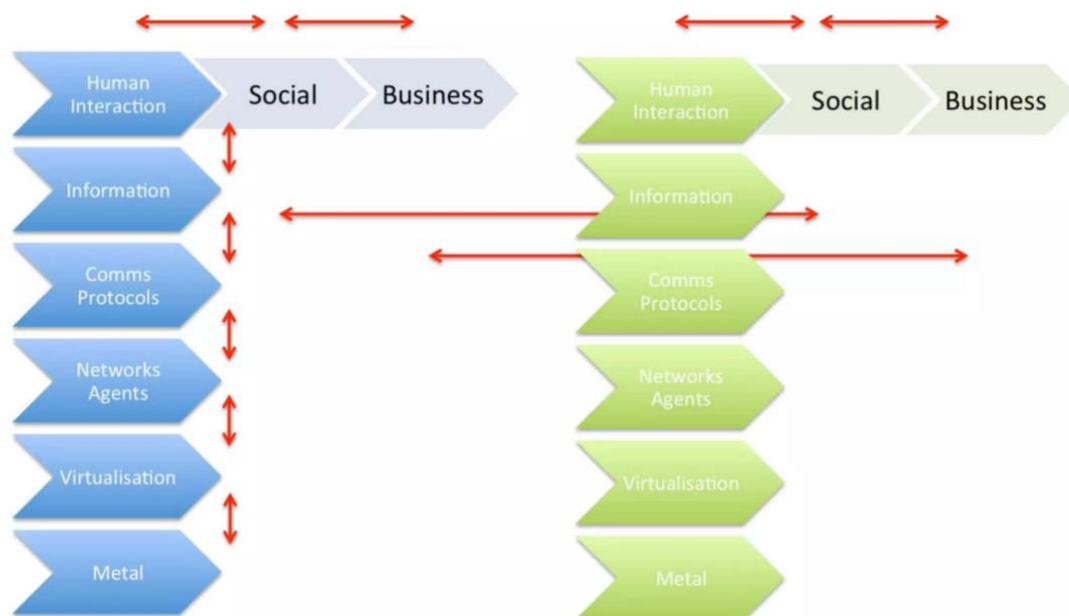


Figure 28: Who trusts who? What trusts what?

In recent years, the concept of Zero Trust has come into play. This drives all actors in the development cycle and supply chain to take measures where trust cannot be ascertained across the complex 5G infrastructure, networks and information exchange systems. Guidelines supporting the application of Zero Trust are found below:

- Technical Guidelines for the implementation of minimum security measures for Digital Service Providers, ENISA 2016⁴⁸;
- Zero Trust Architecture Design Principles 2021⁴⁹.

16.5.2 Testbed viewpoint

The FIDAL security framework considers the cyber risk implication right from the point of gaining physical (or related virtual) access into the infrastructure of the testbed sites and the cascade effect on the business of operating the site. The evaluation will focus on the implication of information breach within the pilot site; the idea is to understand the basic threat level in the testbed site.

Figure 29 illustrates how a physical access by threat actor (someone who represents the threat (malicious or accidental) from the technical viewpoint or gain information regarding the testbed site. The consequence of gaining access to the IT/Virtual components creates vulnerabilities for information breach. The information breach at this level can be of the organisation (security plans, intellectual property, system configuration etc.) or use case information which can have cascading impact on the business operation itself of the testbed operator, partner of FIDAL, or third-party contractor.

⁴⁸ <https://www.enisa.europa.eu/publications/technical-guideline-on-minimum-security-measures>

⁴⁹ <https://www.ncsc.gov.uk/collection/zero-trust-architecture>

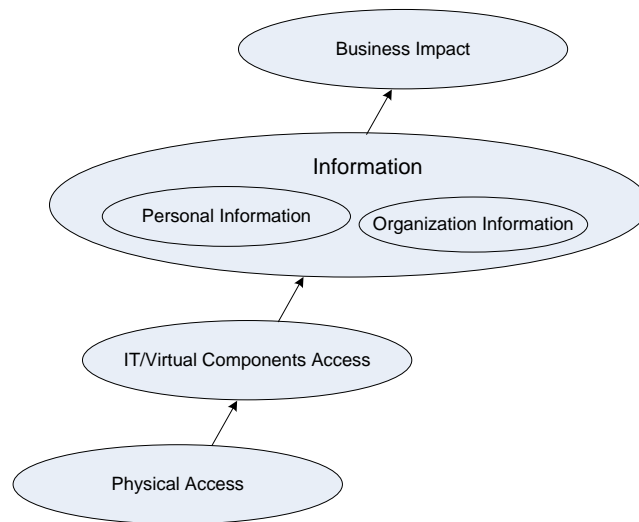


Figure 29: Holistic security view.

16.5.3 Component domain viewpoint

Figure 30 illustrates a set of interconnected component domains. It is common in operational telecoms networks to physically and/or logically separate the IT connectivity to manage the network, from the network carrying application plane (user plane) data. No concept of application (use case) specific data security is illustrated here.

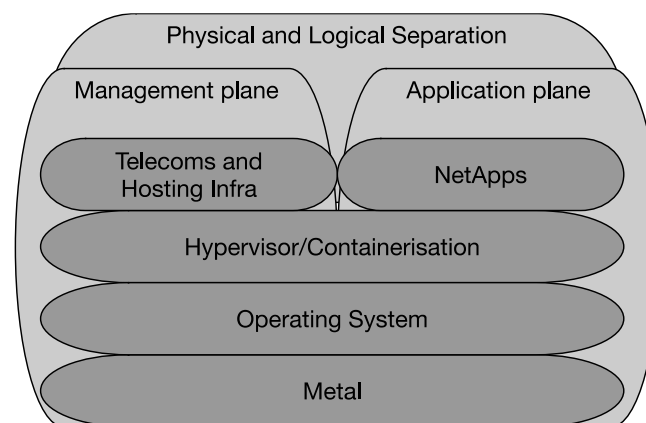


Figure 30: Abstract component domains.

16.5.4 Security from low TRL research, prototyping, field trials to live

FIDAL components are developed in the range TRL5 to 8. TRL5 is a prototype demonstration level. TRL8 is close to live use of the component. TRL's can reflect the maturity of the component, which can also reflect on the level of unknown vulnerability that can be considered in a risk assessment. Components of Low TRL level can be considered to have a higher unknown vulnerability characteristic due to the more limited levels of testing carried out both in terms of code and configuration since the component's lower TRL inception. Higher TRL components can be considered less with less unknown vulnerable as they have likely been through many iterations of test, development, and maturation. CI/CD processes should include sufficient test cases and static analysis throughout the development process. The principle of DevSecOps should be considered to secure the software development process by integrating security early and throughout the software development life cycle.

16.5.5 Delivering for society

As already described in the KVI section, these value themes carry with them specific implications for security. They are further elaborated below:

- **Safety:** Safety refers to the safety of humans and systems. Secure systems are key to this. This requires understanding how new features of a system change the security requirements and foci. It also suggests that discussion with stakeholders is needed as to how priorities should or should not change in response to the introduction of new technology.
- **Sustainability:** Sustainable 6G and 6G for sustainability drive much of the beyond-5G innovation, and encourages processes that support environmental, societal, and economic sustainability. Sustainable 6G suggests that security processes should not impede such developments, by, for instance, requiring greater material or energy resources to be deployed. 6G for sustainability speaks to what 6G technologies can do to better create sustainability. This includes developing solutions in a way that are flexible enough to support digital inclusivity (e.g., that can be used across different regions and socio-economic contexts), that improve community well-being (e.g., by supporting local safety practices and needs), or that improve market access for local businesses (e.g. as security service providers, by not limiting the market access through security practices kept behind IPR), and that support improved environmental practices within local communities.
- **Energy Consumption:** As a subset of sustainability, security processes should not increase energy consumption. Indeed, the project should endeavour to develop security processes that reduce consumption.
- **Trust:** Trustworthy interconnectivity derives from secure systems. This includes systems developed in ways that one system can trust another (in terms of connecting to it, accepting the information from it, etc.) or that components along a lifecycle can be trusted. It also includes users being able to trust a system, which requires a level of understanding and literacy in security features to both make autonomous assessments and to accept the trustworthy signatures provided by a system. There is also the ability of users across a system to trust the security practices that each enact that complement the technical security layers. Finally, there is a layer of societal trust, of the public trusting a user to work in a secure way with a system.
- **Privacy and Data Protection:** defined by both human and data privacy, security has to address both aspects. Security needs to both maintain personal data protection as well as auditability and traceability of actions with personal data to ensure data protection rights. It also needs to ensure human privacy, where activities that could be personally intrusive have the appropriate level of security to ensure human dignity and safety.
- **Accessibility:** All security processes should be accessible to the users. This requires engaging a blend of explainability, understandability, justifiability, and digital literacy. They should also be deployable in the broadest range of contexts as possible (e.g., compatibility with legacy systems, affordable) in order to not limit who gains benefits from the security measures or increase the risk of those unable to deploy such systems.

While incomplete and in-progress, to be revisited and specified with each use-case, in the Table below are a sampling of KVIs that are relevant to security. They show that security—and most importantly the resilience and trust it enables, requires more than just technological solutions.

Table 61: initial suggested KVIs for security.

Value theme	Objective	Enabler	Indicator
Security	Mitigating Vulnerabilities	Threat and vulnerability identification practices (both technological and human)	Ratio of vulnerabilities identified and fixed to safeguard FIDAL's users.
	Delegation of responsibility	processes that delegate responsibility to appropriate parties and ask them to consider their impact to the wider ecosystem.	No. of processes, kinds of processes
	Security preserving	FIDAL security framework and internal processes; use case security evaluation, validation	100% system secured
Responsibility	User Control	User control functions	Ratio of system behaviours users can manipulate

	Accountability	Automated auditability of risk flows	Existence and effectiveness of risk management oversight and control mechanisms, with clear chains of responsibility
Trustworthy	Dependability	User understandable error detection capabilities	100% stakeholders deem system dependable for their activities; Probability of error; Ease identification of error
	Building confidence	Hands-on experience (with risk relevant synthetic data)	% opinion decrease in risk, from survey responses on reported confidence.
Transparency	Explainability	User-friendly security trainings and hands-on use-cases	Survey, user questions that demonstrate literacy and assessment capabilities
Safety	Engaging emerging technology to improve safety and security of information and services	AlaaS	Number of security risks for which AlaaS can support users in threat identification
	Support accreditation/verification of vendors and systems	Assessment of security via standards and guidelines	Number of recommendations for requirements for accreditation/verification.
	Feeling safe	Opportunities to test the security realism of whole use-case systems (blending organisational and technological practices)	Number of opportunities per use-cases; Survey of user perception.
	Risk Management	Development of risk analysis points as part of monitoring mechanisms	No. of high-risk paths found and mitigations deployed
	Easy to use tools	Survey, users find tools easy and self-explanatory	% of survey response pos./neg.
Economic Sustainability	Supply chain sustainability	Bill of Materials for supply chain management	Ratio of supply chain for which there are and are not Bill of Materials or related certification of sourcing.
	Improved supplier market entry potential	Development of (re-usable) security patches or other off-the-shelf security components	Number of UC relevant patches/components that can be applied both within the project and to other tools
	Identification and implementation of new human-centred security service opportunities.	Security API to access to measures; Automation/adaptation flexibility, resilience measures	Fulfilment of Zero Trust measures No. of new processes accessible to outside suppliers (e.g. open calls)
Data Protection	Personal Data Protected	GDPR compliance	100% personal data protected from unauthorised use.
	Accountability	Security practices that consider both technological and human components	100% of providers/services have accountability mechanism in place (both technological and organisational)
	User Control	Human-in-the-loop design	100% user control over personal data (as appropriate to rights)
Business Value	Solve existing and emerging problems	Development of (re-usable) security patches	Survey, stakeholder perceptions of problems solved (fully or partially)
Environmental Sustainability	Reduction in energy consumption	Energy efficient components and analysis (proportionate methods for security)	% energy use reduced (predicted, calculated in trial)
	Does not hamper the development and deployment of a low-	Flexibility in security technology	Comparative low power solutions with equivalent security capability

	carbon alternative (e.g. does not lead to lock-in of current emissions)		
	Increased lifespan via reparability, upgradability or reusability of products	Ability to update security measures, ability to repair despite security requirements	Periodicity of repair, upgrade, reuse events

16.6 FIDAL Security Methodology

FIDAL's security methodology starts with building a culture of security across the project. This is not a rule book to be followed, but rather a methodology to be appreciated by all partners. The methodology is founded in a key assumption: that all partners have suitable organizational policies and suitable experience. The methodology first sets out how security applies to different process contexts within the project (Trials, Network Applications Development, Network Applications Deployment, and Testbed development and operation). It then describes the current security awareness and practices across the project partners. It then discusses key goals of security: building trust and ensuring resilience. It follows by elaborating the specific needs of the project as a whole, and the PPDR and Media verticals in specific, with a specific focus on AI security requirements. The security process that builds upon this security culture is elaborated in Chapter 16.7.

16.6.1 Security in different project contexts

Figure 31 illustrates key factors of the FIDAL Security Methodology in the different context. These include:

- **Trials**
 - Security risk factors are determined during development and deployment and in preparation of the trials.
- **Network Applications Development**
 - Network Applications are developed from new code with dependencies on existing code and interacting components.
 - Functional testcases and static analysis should be automated in the CI process.
 - FIDAL Open Calls should encourage software quality and assess the security capability of the provider.
- **Network Applications Deployment**
 - Where Network Applications are deployed with functional test cases that appropriate fit the testbed for deployment and are modified as the testbed evolves.
- **Testbed Deployment and operation**
 - Supply chain security must be assessed during procurement of testbed components.
 - Component configuration must be carefully assessed to ensure minimum vulnerability presented by the testbed components.
 - 3GPP security features must be appropriately enabled and configured.
 - Change management must be followed for component configurations.
 - DevOps/DevSecOps (CI/CD) tooling should be implicitly secured. Vulnerability here will reflect on all components which are dependent on the CI/CD processes provided.

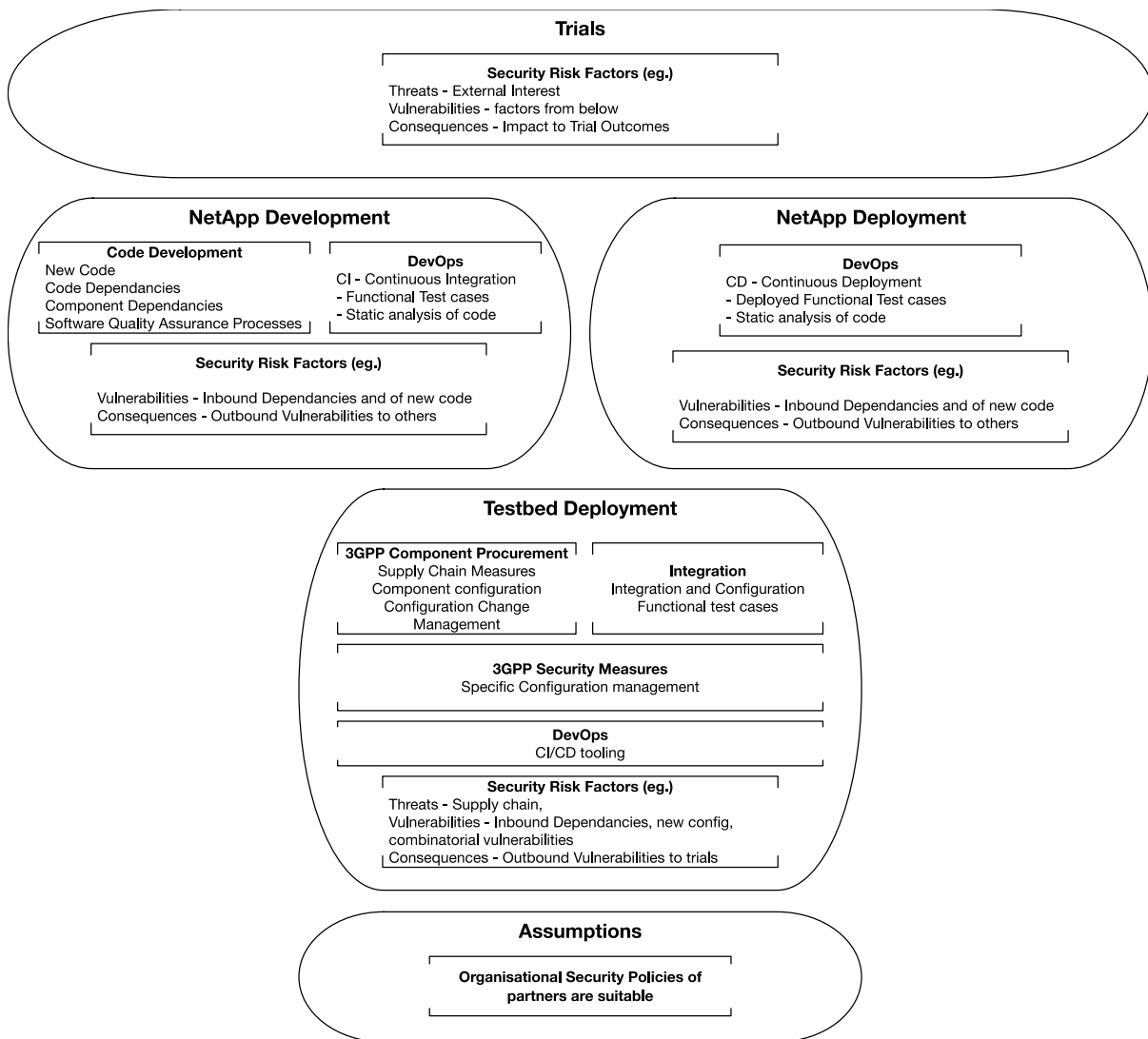


Figure 31 Components of the FIDAL security methodology.

16.6.2 Security Awareness across the project

FIDAL partners understand security as addressing three aspects: people, processes, and technology. By ensuring that both developers and users are knowledgeable and security-conscious, implementing robust processes, and deploying secure technologies, FIDAL can create more resilient and secure solutions and environments. The FIDAL security declaration, guidelines and assessment will increase insights, risk awareness and maturity level as the project progresses, with revised assessment rounds likely needed.

Partners bring a mix of security foci, with some focusing primarily on the security of technology (software vulnerability, robustness), some on the security of people (e.g., confidentiality agreements, physical access to testbeds, ability to bend rules, organisational requirements), and others on information processes (e.g., data exposure, particularly personal data or through information exchange between partners). As the solutions and UCs take shape, the project’s security processes will need to be further specified to support partners in thinking about security as a human-centred technology process, where people, process, and technology work together to make security in specific contexts, situations, and goals.

Current Security Practices and Foci

FIDAL partners’ security practices are based in confidentiality, integrity, and availability. Availability (of network to perform trials, uninterrupted access, and connectivity) is a key driver and motivator for partner security practices. Confidentiality encompasses protecting information from being accessed by unauthorised parties during an experiment. Integrity centres on secure and protected data transmission. To minimize risk prior to assessment, secure

and strong authentication and authorisation procedures are already in place across the components, the use of critical components is limited to a sub-set of personnel with appropriate credentials, and auditable access logs are maintained. One partner also engages with RBAC and VPN solutions to limit risk. Informational risk processes include secure data handling, minimising sensitive data collection and retention, anonymizing when possible, and using encryption mechanisms for sensitive data protection at rest and in transit.

Risk assessment

Acknowledging the unique configurations and contexts across the UCs, partners currently assess security risks processes per case and if one is identified develop an experiment to test and mitigate it. Risk assessment will be harmonised across the project.

Software Development

Partners developing software engage in quality and security assurance measures including:

- Separating development and deployment environments
 - Developing the software in a firewalled environment, separate from real-world deployment.
- Staying up to date
 - Keeping current with security and QA guidelines.
 - Ensuring all programs, frameworks, and libraries are latest versions.
- Internal testing and uniformity practices
 - Internal robustness testing (of various degrees and styles, including on SQL injection, cross-site scripting, engaging static code analysis tools).
 - Some partners follow Test Driven Development while others engage in unit testing to proactively and with agility identify and address security concerns.
 - Engaging checkstyle rules to verify that code formatting is universal across the team.
- Protecting data processing and movement
 - Encryption mechanisms to protect data transmission.
 - Authentication/authorisation system for user identity verification.
- Data protection practices where required for the UC
 - Privacy protection through personal data anonymization.
 - Data deletion after the project or per user request.

DevOps CI/CD processes

Partners engaged in DevOps CI/CD processes for component development employ security mechanisms to identify potential security vulnerabilities in ways that support the greatest chance to be patched.

- Limit the dependencies to third-party libraries.
- Use the latest compatible dependency for a given software.
- Follow the recommendations for security vulnerabilities proposed by github (for processes on github).
- Use pre-configured Jenkins pipeline that includes vulnerability scanning using Sonarqube.
- Engage deployment pipelines with verification and validation processes against CAPIF.

16.6.3 Building trust across and beyond the project

Trustworthiness carries a rich range of definitions for FIDAL, relevant to the diversity of partner contributions and experiences. Section **Error! Reference source not found.** illustrates the complexity of the different dimensions of trust.

Trustworthiness can imply confidence, assurance, dependability, certainty, reliability, credibility, and integrity. It can reference systems, organisations, processes, or people. It can further be defined by the source, timeliness, and the importance of information, where truthfulness and correctness also become criteria. The diversity of definitions also

suggests the need for clarity and agreement along the way to ensure the technical, informational, and human aspects of trust are fittingly addressed in ways that support human-centred security needs.

Negative factors affecting user trust include:

- Understanding the risks of off-the-shelf components/code.
- Much technology is currently adapted to consumer security needs and not those of PPDR.
- Users engage with interfaces that do not always (nor should always) show the risks associated with what is connecting them.

Trust is not a one-time assessment but an ongoing process that requires periodic reassessment and verification. Engagement with end-users to understand how technological development and organisational practice inform each other needs to be iterative and continuous. Trust can be evaluated via people's attitudes (e.g., surveys), via technical security standards of a system that are enforced (e.g., via KPIs showing consistent behavior of both apps and their results in the testbeds), and via identification of organisational processes (e.g., via internal metrics or observations). Previous experience with the person/party/company/tool and knowledge of prior success stories can play a large part in establishing trust, where attitude and consistency in delivering on their promises and most importantly their willingness to participate in solving sudden issues and/or problem become additional criteria.

What is done during the project also impacts beyond the project. For example, improving explainability and understanding of security enablers for users is key for when they lose direct access to developers and have to make trust assessments themselves. Activities to build trust beyond the project can include, during the project:

- developing training and repository of services around security.
- interactions during the project to build strong basis for future trust.
- Working by partners to gain a deep understanding of trust drivers and enablers during the project can support improved definitions, design, and explanations afterwards.

16.6.4 Building resilience across and beyond the project

Resilience “is a measure of a system's ability to retain its originally intended performance after being compromised”.⁵⁰ Compromise could be in the infrastructure, wired and wireless communication bearers, virtual components, physical networking, virtualisation hardware, and data transfer activities. Information being carried within the infrastructure must be secured in a way that does not rely on the infrastructure for that security. These elements intertwine and shape trust (e.g., software trust hardware, hardware trust software, user/provider trust both). Thus, FIDAL will develop a robustness rational and service level agreement that supports resilience, relevant to the UCs requirements. A security approach and architecture in support of this will be established for reuse within and across the test beds.

However, currently, there is a lack of processes and mechanisms to enable fit-for-purpose security validation across the supply chain, 5G security requires different skillsets than previous forms of connectivity, and there is limited education or training to support formations of security strategies. With the influx of standards in the area without strong guidance as to how to prioritise them, FIDAL will:

- Focus security activities, as a priority, on what needs to be protected in a use case and what matters about that protection (e.g., is it availability of information, integrity of interactions, confidentiality of systems). These activities will need to be continuously re-evaluated and re-validated throughout the project to ensure fit for purpose and effectiveness.
- Engage telemetry and AI to support monitoring and detection of threats as well as to automate (when appropriate) mitigation, validation, and certification measures and methods.
- Integrate technology across use-case architecture in ways that support end-to-end view of system and data integrity.

⁵⁰ Rhodes et al. (2015) 5G innovation opportunities – a discussion paper. Future Technologies Network. Available at <https://repository.uel.ac.uk/item/85005>, p. 59

- Where possible, engage network slicing as a component of security.

These actions will be supported through the exchange of information between the testbeds and the common repositories to evaluate and compare results (for improvements).

Any resilience plan also needs to consider business continuity plans within and beyond the project. FIDAL will build a plan for scalability and flexibility that accommodates future growth (increased demand, geographic resiliency) and changes in project requirements, allowing the designed platform to easily adapt and scale without compromising performance or security. For example, automation can, during the project, focus on automated configuration, deployment and testing (e.g., resource reallocation) to ensure service continuity. For after the project, a focus on automation of software components deployment will add to the resilience beyond the project since components will be easily swappable in Testbeds and production infrastructures (post the project's lifespan). This will entice more developers to use FIDAL's infrastructure, prolonging its lifespan.

Risk from mobile outage

Emulating a mobile network where there will be a loss of mobile connectivity is particularly relevant for the UCs yet poses a challenge for FIDAL, thus future security risk assessment practices need to ensure resilience is both component and UC appropriate (e.g., emulate mobile networks in the test environment with testing equipment from vendors such as Spirent or Keysight to reproduce Network conditions during tests).

16.6.5 Maintaining a Library of Security Controls

In FIDAL, we will maintain a library of security controls. This represents where security measures are put in place during component development and testbed integration and will be updated during the project where mitigations are implemented in response to a risk identified during the risk management process.

In this library we will identify the following non-exhaustive list of factors:

- Known Vulnerabilities and patches,
 - leveraging public records of known vulnerabilities (e.g., Mitre CVE⁵¹)
 - regular software updates
- Known secure configurations:
 - Classical IT components
 - Telecom specific components
- Reference to publicly available national and international guidance
 - ENISA topics⁵²
 - GSMA Knowledgebase⁵³
 - National guidance from CSIRTs e.g., UK National Cyber Security Centre⁵⁴
- Project specific learnings and fixes

There will be a process of disclosure and recording in the project where partners will be encouraged to share knowledge of security vulnerability and mitigations. Where specific learnings are not yet found publicly, then measures will be taken to disseminate that through appropriate disclosure methods. Disclosure methods may not be fully public, such as GSMA Coordinated Vulnerability Disclosure (CVD) programme⁵⁵.

⁵¹ <https://cve.mitre.org>

⁵² <https://www.enisa.europa.eu>

⁵³ <https://www.gsma.com/security/5g-cybersecurity-knowledge-base/>

⁵⁴ <https://www.ncsc.gov.uk/section/advice-guidance/all-topics>

⁵⁵ <https://www.gsma.com/security/gsma-coordinated-vulnerability-disclosure-programme/>

For information, ENISA provides CIRAS, a useful, but anonymised, visualisation of breach notifications.⁵⁶ This is useful for general awareness, but unlikely useful for FIDAL detail.

16.6.6 Specific needs of the project

Existing Security Concerns among partners and UC include:

Testbeds:

Testbeds raise a particular security challenge for FIDAL, where security is blended between organisational and technical aspects. Concerns exist around unauthorized access and installation of harmful software along with the integration of network applications.

Partners internal security processes to mitigate these risks include clearly defining the security requirements and objectives for FIDAL's network application, including aspects such as data confidentiality, integrity, availability, access controls, and secure communication. In addition, partners consider guidelines and recommendations from reputable sources, such as the vendor documentation, security organisations, or industry-specific standards. Operational monitoring of testbeds is currently done by a mix of 24h monitoring and alerts for strange traffic spikes and resources usage, random traffic monitoring, which would need to be consistently decided upon across the project and proportionate to risks. Partners complement these mechanisms with software tools such as Kubernetes (to manage cluster deployments), Docker and Helm Charts (to manage singular or multiple container deployments), Terraform for managing Infrastructure as code, and Ansible for configuration of services. When possible, files are stored in Github or GitLab to control changes. Partners also support organisational aspects by, for example, removing default passwords or for deactivating interfaces that are not necessary.

Use Cases

Uses Cases in particular raise security concerns for FIDAL, including:

- Security in a multi-tenant infrastructure
- Unauthorised access (to the network applications, software, core datacentre, hosting the 5G SA Core, other critical entities)
- Onboarding of harmful software, e.g., through Open Calls
- Man-in-the-middle attacks on the connections between UEs, edge nodes and cloud making available the eavesdropping of sensitive data
- Lack of necessary bandwidth and improper latency lags leading to system malfunction
- Connection loss or degradation between the software running on UEs and the cloud services, prohibiting this way the necessary communication with cloud services
- Confidentiality, network and services exposure, integration with the testbed services
- Data security, Network security, User authentication, Incident response and recovery

Open Calls

Open calls raise unique security concerns due to the integration of outside, less directly controlled components into the FIDAL testbeds. Thus, they need special security considerations, potentially built around a zero-trust approach, to be considered both within the projects internal guidelines (as security policies and procedures) as well as the open call criteria.

Considering this, the security policies and practices will be among the criteria for proposal and results evaluation. This can include:

- how the applicant manages access control
- how the data is protected
- incident management; how potential vulnerabilities are tracked, identified and corrected

⁵⁶ <https://ciras.enisa.europa.eu>

- security incident history (recorded past security incidents)
- adherence to standards and best practices.
- data protection and privacy procedures, particularly when UC require sensitive data handling, storage and encryption.
- other regulatory aspects and ethics guidelines considered.

16.6.7 Needs of the verticals

PPDR: PPDR raises unique priorities in security risk assessment and mitigation, engaging particularly sensitive contexts. In crisis situations, network availability is vital both for mission critical communications and public trust.

- **Security of mobile Infrastructure and IoT:** part of critical infrastructure, with supply chain interdependence of other actors such as utilities (power generation/distribution, intelligent transport), resilience across this complex connectivity is paramount. System robustness, here, is equally important to security as mitigating cyber vulnerabilities. Network isolation, device identification, secure communication can all support security.
- **Processing sensitive and personal information of the public:** such as information handled by the Emergency Services, Health Care, which requires additional levels of security, data protection, privacy, and ensure security measures maintain the dignity of the public affected by the emergency. Any service layer interfacing (e.g., of health, fire, police, public, private, etc.) raises heightened risks. Network, physical, onsite, and cloud security are all required.
- **Dynamic security needs:** security needs change over time, quickly, as a crisis progresses, prioritising different security requirements at different stages of an emergency. Related, as PPDR practitioners move around to address the emergency, they could face new service conditions and unknowns regarding MNO interfacing and switching to other carriers. PPDR use case security strategies require liaising early to understand interdependent security and policy requirements. This poses a particular challenge for automated security processes, which on the one hand relieves PPDR practitioners from having to think about security of their systems while they engage in securing the safety of their communities, but also does not always support the diverse security arrangements raised by each new crisis.
- **Safety of PPDR personnel:** on the scene, putting their lives at risk, security needs a strong focus on its human impact, appropriately balancing security of a system with security of the person.
- **Supply chain security:** ensure accountability of the security and privacy levels across the supply chain, maintaining the sensitive needs of PPDR at all points within its lifetime. These supply chains, and related materials, ICT systems and apps need continual monitoring during development and lifetime use. Similarly, this requires the ability to assess how politics could affect component choices, downstream IP, and sovereign control.
- **Physical damage:** emergencies often come with physical damage to infrastructure (e.g., mast or sensor damage), pointing to the need for physical security practices paired with cyber security.
- **Identity and access management:** to support only those with appropriate rights and verified identities to access services and resources at the right time for the right reasons.
- **Connecting with legacy systems:** PPDR have existing systems and processes which need to remain closed. Thus, new tools will likely have to open their API to these systems, requiring trust signatures.

Media: Media, as a vertical, comprises of public services, big data, surveillance capabilities, large-scale venues, private companies, private spaces, as well as artistic and cultural systems. This complex multi-layered context makes security concerns particularly challenging to predict.

- **Security of smart infrastructure:** unauthorised access can realise critical infrastructure vulnerabilities such as water system hacking or electricity shut off, posing threats to system's reliability and safety. Network, physical, onsite, and cloud security are all required. This needs to be complemented with the ability to develop a routine risk assessment strategy and mitigation plans related to the entire supply chain from sensor development and deployment to integrated human and technology internal processes to manage access installed sensors.
- **Security of personal, public service, and business data:** unauthorised access to media services can lead to personal data breaches as well as reveal sensitive business practices, posing a threat to privacy and business

continuity. This requires system security processes, from encryption to anonymisation. In places, automation processes can improve these security processes (such as logging access and actions).

- **Content security:** related to the above, media carries with intellectual property, which can be stolen. Additionally, audiences can experience gaps in quality of services posing a threat to economic sustainability and growth. This requires protection of physical servers, data transmission routes and related connectivity infrastructure as well as organisational security practices that enable and limit human behaviour.
- **Protection of persons:** Access to large scale media systems can reveal the positions and presence of large public groups or even select individuals, posing a threat to their safety, wellbeing, and dignity. This involves development of improved risk visibility processes that support security assessment teams and auditors to identify threats, vulnerabilities, and impacts of different mitigation measures taken. Transparent (if securely distributed) documentation can further support these efforts.
- **Public access and interfaces:** in some use cases, the public can access or post content, affecting what kinds of security protocols can work across the diversity of public devices. This additional traffic expands the security threats, vulnerabilities, and who experiences the consequences (e.g., uploaded or downloaded malicious content, hacking, affects simultaneously private individuals and public services). Encryption, filtering, and access rights are all necessary.

16.6.8 Risk based approach to AI

The general black box nature of AI, where incorrect behaviours are difficult to anticipate, detect and/or debug, raises great security concerns. This, in part, comes from the lack of control regarding the algorithm's training, output, quality, consistency, monitoring, and existing biases in the training data. This can be exacerbated by difficulty in identifying responsibility after a harmful outcome (along with potential lack of accountability and self-reflection in the involved persons, both users and developers). This is particularly relevant in systems that involve decision-making processes, especially automatic ones. Identifying and addressing these potential errors or unwanted system behaviours can be very resource intensive. Concerns, thus, exist about the integration of AI with the rest of the components in FIDAL. AI in FIDAL is planned to be leveraged 'as a service', therefore it has to be modelled so that it can be used by the other modules whenever needed. Modelling a versatile feature such as AI can be challenging. Similarly, ethical challenges can arise, for example around service denials, that raise novel forms of bias mitigation requirements.

Consequently, AI components used in the FIDAL project must be risk assessed following the approach provide by the EU Artificial Intelligence Act which is illustrated in

Figure 32.

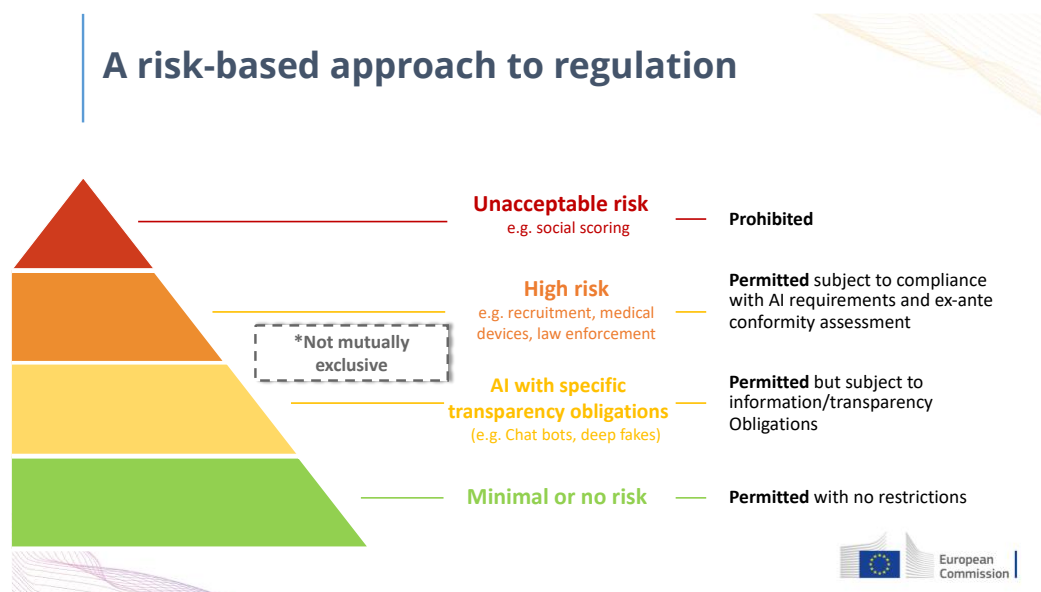


Figure 32: EC Risk based approach to AI Regulation⁵⁷.

AI - Measures to protect AI as a Service (AlaaS)

Adversarial Machine Learning (AML) is a class of data manipulation techniques that cause alterations in the behaviour of Artificial Intelligence (AI) systems while going unnoticed by humans. These alterations can cause serious vulnerabilities to mission-critical AI-enabled applications and specifically to APIs serving AI models. These vulnerabilities may include either data poisoning which has an impact onto the training of the model, or data evasion which has an impact onto the weights of the AI model and thus the way it produces its results. Within FIDAL, we will investigate the case of robustifying the AlaaS capabilities by augmenting the datasets with adversarial examples to safeguard, secure, and make the AI systems more reliable. The need arises from the fact that Neural Networks are as good as their data. At the same time, data may be prone to inherent distortion, noise, and errors. The challenges posed by AML have recently attracted the attention of the research community, as possible security issues on AI systems which can pose a threat to systems reliability, productivity, and safety.⁵⁸

In this context, there is a pressing need for robustifying the AI models against diverse perils of adversarial attacks. The research and development efforts need to be intensified and drill into the details and the specificities of existing AI systems, investigate their vulnerabilities, and introduce solutions that make machine learning (ML) and deep learning (DL) models more resilient against adversarial inputs, attempts of poisoning, and evasion attacks. To tackle these security aspects, in FIDAL we will devise different adversarial techniques by extending the work of Anastasiou et al. (2022), including adversarial training and defence algorithms to investigate their applicability and effectiveness under real networking conditions.⁵⁹

AI used for assisted situational awareness

State of the network: AI will be used to monitor and adapt the configuration of testbed networks to optimise their function. Risk will be assessed to consider the scope of human notification and intervention so as to not artificially create network inefficiencies and outages.

Use case specific: AI Network Applications may be used in the User plane as an example of the benefit 5G capability to improve the Use Case.

- PPDR: AI may be used to improve a response situational awareness. It is unlikely that live data will be used, so we expect risk to be low.
- Media: AI may be used for content object classification, manipulation and/or creation. For example, identifying age related content.

16.7 Security Processes

Here we summarise some of the processes in the FIDAL Methodology.

16.7.1 Supply Chain considerations

All partners shall be aware of the concerns of supply chain risk as stated in the 5G Toolbox, and the declaration made as illustrated in the DoA which is presented in section **Error! Reference source not found.**. Open calls will require to communicate the Horizon Europe declaration (section **Error! Reference source not found.**) and ensure that the FIDAL partnership can continue to honour that declaration.

16.7.2 Security Accreditation and Certification

⁵⁷ Taken from the presentation of Yordanka Ivanova, Legal and policy officer European Commission, DG Connect. Presented at PSCE Forum Conference on 30 November 2021: <https://www.psc-europe.eu/psce-conferences/brussels-2021/>

⁵⁸ Bécue, A.; Praça, I.; Gama, J. Artificial intelligence, cyber-threats and Industry 4.0: Challenges 669 and opportunities. *Artificial Intelligence Review* 2021, 54, 3849–3886.

⁵⁹ Anastasiou, T., Karagiorgou, S., Petrou, P., Papamartzivanos, D., Giannetsos, T., Tsirigotaki, G., & Keizer, J. (2022). Towards Robustifying Image Classifiers against the Perils of Adversarial Attacks on Artificial Intelligence Systems. *Sensors*, 22(18), 6905.

This will not be primary goal for testbeds such as in FIDAL, but all partners should be aware of Accreditation and certification schemes in order to safeguard future adoption of solutions:

- ENISA Certification⁶⁰;
- GSMA Security Accreditation Scheme⁶¹;
- Common Criteria⁶².

16.7.3 Software Quality

Awareness will be drawn across the project, and guidance provided, towards the importance to follow software quality processes and procedures. This is outlined in section 16.5.4 in the context of low to high TRL, and is placed within the overall methodology explained in Section 16.6.

Examples of public materials include:

- Secure Software Engineering Initiatives⁶³;
- ADVANCING SOFTWARE SECURITY IN THE EU: The role of the EU cybersecurity certification framework⁶⁴;
- From candidate to certification⁶⁵;
- Use of Static analysis⁶⁶;
- Common criteria⁶⁷.
-

16.7.4 Operational monitoring

Details of operational monitoring will be collected from testbed operators to seek the possibilities to detect anomalous activity in the system. This can then be used to reassess risk (please refer to Section 16.7.5).

16.7.5 Manual Risk Assessment

The primary approach in the FIDAL Security Methodology is risk management centric, where we seek to establish and keep a risk register up to date. The security approach of FIDAL will be bottom-up. It should start with components and interconnect. Then move on to networking and information flows. The participants know their own information and technology assets. They will have their own view on security and will help prioritise security risk and implement mitigating actions. Our risk assessment process consists of two work streams:

- A technical assessment - Technical vulnerability/risk presenting vulnerability to information assets.
- An information assessment - Information flow vulnerability and risk based on business needs.

For FIDAL, the technical assessment will be most important. The information assessment is not considered to be important as the FIDAL solution is not intended to carry live information. This will be considered for cases where the full solution is tested, and where there is potential for live information exchange with COTS UE's.

Our approach to risk assessment is more lightweight than ISO27005, or NIST risk standards. We base our risk management approach to the more generic ISO 31000, which is then utilised in context for the FIDAL project.

This approach has been used within Horizon 2020 '*Management Of Networked IoT Wearables – Very Large Scale Demonstration of Cultural Societal Applications*' MONICA project⁶⁸, and builds upon work of the FP7 project '*Preventative Methodology and Tools to Protect Utilities*' PREEMPTIVE⁶⁹ including foundational work in Physical Security risk, documented for DG Energy in 2010: Reference Security Management Plan RSMP⁷⁰.

⁶⁰ <https://www.enisa.europa.eu/topics/certification>

⁶¹ <https://www.gsma.com/security/security-accreditation-scheme/>

⁶² <https://www.commoncriteriaportal.org>

⁶³ <https://www.enisa.europa.eu/publications/secure-software-engineering-initiatives>

⁶⁴ <https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework>

⁶⁵ <https://www.enisa.europa.eu/topics/certification/from-candidate-to-certification-scheme>

⁶⁶ https://owasp.org/www-community/controls/Static_Code_Analysis

⁶⁷ <https://www.commoncriteriaportal.org>

⁶⁸ <https://www.monica-project.eu/home/about-monica/>

⁶⁹ <https://cordis.europa.eu/project/id/607093>

⁷⁰ https://energy.ec.europa.eu/system/files/2015-01/2010_rsmp_0.pdf

UK DCMS 5G Testbeds and Trials funded projects also use the same methodology:

- UK DCMS Mobile Access North Yorkshire (MANY);
- UK DCMS 5G Factory of the Future (5GFoF).

The following risk assessment approach (Figure 33) was shared with partners at the Kick Off meeting:

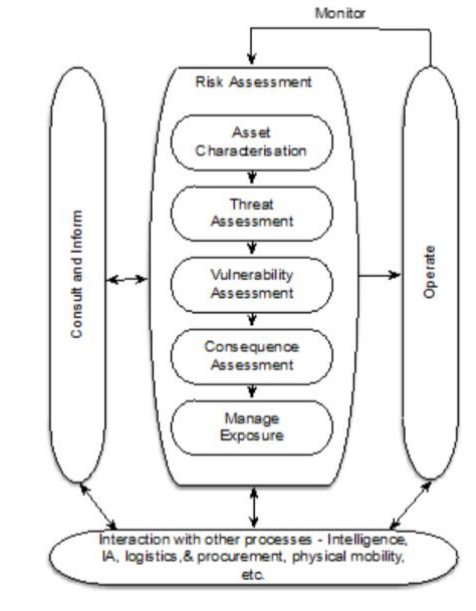


Figure 33: Risk Management approach.

In risk assessment traditionally, information security focuses on confidentiality, integrity and availability, but a change in culture is needed and security should be more approachable. Overthinking leads to “too much” security, and vice versa. In our approach we ask: “what needs to be secure, and why?”. Bearing in mind that the wider threat context includes political threat, commercial threat (IPR), and the related threat intent and capability.

In FIDAL, the risk assessment should be co-created and peer reviewed. Noting that documentation is only useful if it is understandable. Partners will be reading each other’s documentation, and that we propose to document component interconnect and information flows using [ArchiMate](https://www.archimatetool.com)⁷¹, open- source software. This serves to identify components, associated Intellectual property (considering supply chain factors) and their link to risk factors. Risk factors are illustrated in Figure 34. Our risk methodology can scale accordingly to the scope of the factor to be assessed.

⁷¹ <https://www.archimatetool.com>

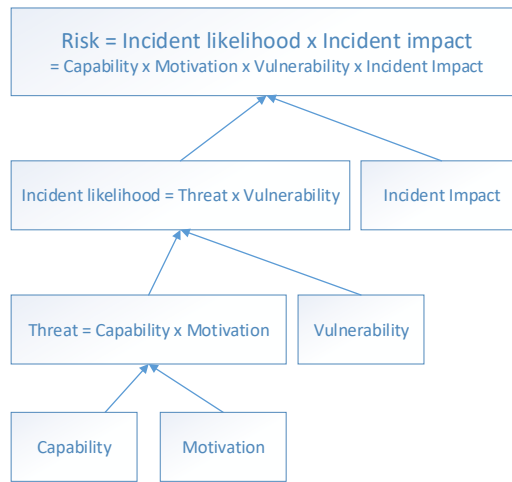


Figure 34: Factors of risk assessment.

Figure 35 illustrates a 2-step approach to risk where Technology and Information flow and considered individually. For technical risk, all components of the testbeds are considered. The Information flow represents the information that may flow during trials. This is especially important if live data includes operational data and/or personal data.

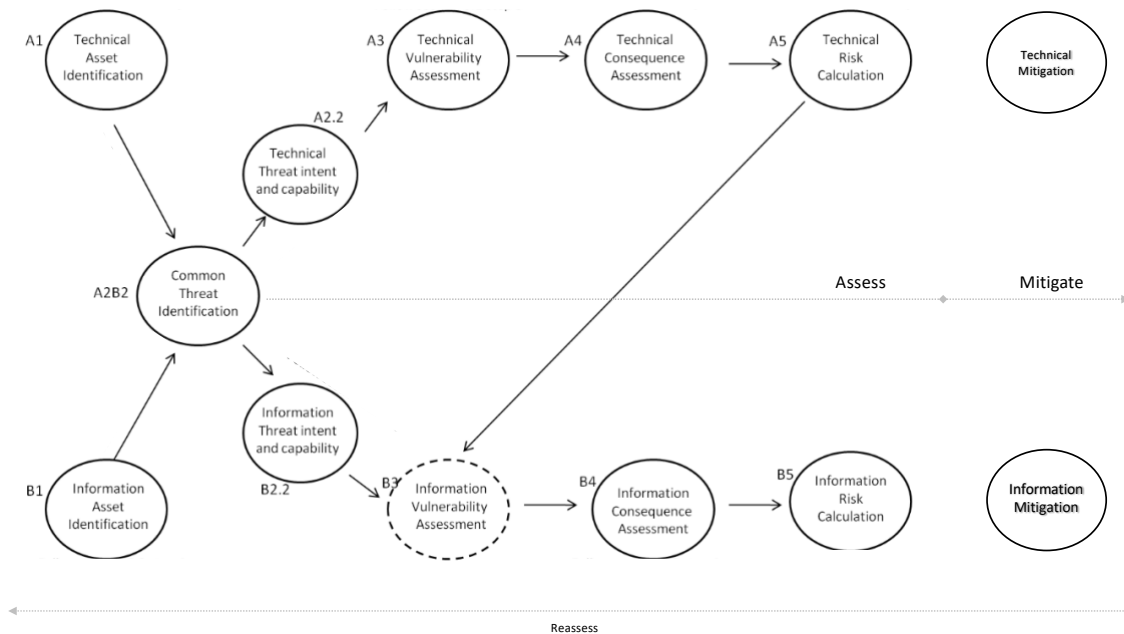


Figure 35: Interdependent risk assessment on the technical and information layers.

16.8 Summary and Conclusion of the FIDAL Security Methodology

In Summary, as described throughout this section the FIDAL Security Methodology will evolve including the following:

- Developing a Structured Security Framework for evolved 5G and 6G, centred on risk management processes.
- Fostering the culture of
 - Software quality and supporting DevSecOp processes.
 - security aware network management.
- Open Call selection and monitoring criteria
 - Working on the zero trust principle.

- a build of the trust relation between FIDAL partners and the external parties engaged.
- A shared awareness across the project of
 - Technical Network security and network application specifics.
 - UE security and UE application specifics.
 - Network Federation considerations.
 - AlaaS security risk.

17 Conclusion

This deliverable presented the in-depth analysis conducted by the project consortium on the use cases within the FIDAL project scope, which are expected to have a transformative impact on the future of 5G networks and applications. The analysis aimed to identify the key stakeholders and their respective roles in each use case, capture stakeholder requirements, determine the technical and business Key Performance Indicators (KPIs), establish the desired targets for those KPIs, and define the necessary measurement methodologies.

In performing the use case analysis, the project took into consideration the most recent recommendations on beyond 5G technologies and KPIs from the 5G-PPP (5G Infrastructure Public Private Partnership) perspective.

Furthermore, this deliverable provides an overview of the work accomplished during the initial phase of the project, focusing on the requirements elicitation, the security implications, and the design of the overall architecture of the experimenters' platform. It outlines the various components that comprise the platform and identifies their integration points within the system.

It's important to note that this deliverable represents the initial version submitted for the first phase of the project and will undergo continuous updates to ensure compliance with high standards. These updates will incorporate feedback from technical reviews as well as insights gained from subsequent tasks and activities within the project.

18 References

- [1] A. C. a. C. S. R. M. P. K. Thiruvassagam, "Resilient and Latency-Aware Orchestration of Network Slices Using Multi-Connectivity in MEC-Enabled 5G Networks," *IEEE TNSM*, pp. 2502-2514, 2021.
- [2] P. B. L. M. I. H. H. Nesse, "Validation of 5G use case solutions - Simultaneous assessment of business value and social acceptance in early stages of the research and innovation projects," *Nordic and Baltic Journal of Information and Communications Technologies*, vol. 1, pp. 37-72, 2023.
- [3] R. Cooper, "Agile-Stage-Gate Hybrids: The Next Stage for Product Development," *Research-Technology Management*, vol. 59, no. 1, pp. 21-29, 2016.
- [4] R. Cooper, "Idea-to-Launch Gating Systems: Better, Faster, and More Agile," *Research-Technology Management*, vol. 60, no. 1, pp. 48-52, 2017.
- [5] K. Still, "Accelerating Research Innovation by Adopting the Lean Startup Paradigm," *Technology Innovation Management Review*, vol. 7, no. 5, 2017.
- [6] L. N. P. D. G. A. O. C. D. P. M. P. Briguglio, "Business Value and Social Acceptance for the Validation of 5G Technology," *IEEE International Mediterranean Conference on Communications and Networking (MeditCom)*, 2021.
- [7] E. Ries, *The Lean Startup: How Constant Innovation Creates Radically Successful Businesses*, Penguin Books Ltd., 2011.
- [8] M. B. e. al., "Ultra-reliable and low-latency communication: Tail, Risk and Scale," *IEEE*, vol. 106, no. 10, 2018.
- [9] C. G. K.-T. C. G. S. P.-C. W. C.-H. H. M. Abdallah, "Delay-Sensitive Video Computing in the Cloud: A Survey," *ACM Transactions on Multimedia Computing, Communications, and Applications*, vol. 14, no. 3s, pp. 54:1 - 54:29, 2018.
- [10] 3GPP, "Service requirements for the 5G system (Technical Specifications)," 2023. [Online]. Available: <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3107>.
- [11] ITU-T, "Vocabulary for Performance, Quality of Service and Quality of Experience," 2017.
- [12] N. TOMs, "Social VALUE Calculator," 2019. [Online]. Available: https://drive.google.com/file/d/1Mfr3GweuxevzQH8CEtfIXLP3UGS_yXi9/view.
- [13] "Wellbeing of Wales: national indicators," [Online]. Available: <https://www.gov.wales/wellbeing-wales-national-indicators>.

Annex I:

A. Standard Network KPI Definitions

This section presents standard network KPIs as defined for 5G networks, including target values set for the 5G system. The definitions of the KPIs and how they are evaluated will be reused for B5G and 6G but the target values will be updated. In this section the KPIs are described along with 5G target values - new target values for B5G and 6G are proposed in the following Section based on input from ICT-52 projects. The KPIs from standards covered in this section are selected based on presence of related KPIs from ICT-52 projects, meaning that some KPIs previously described in standards are left out, e.g., KPIs related to mobility.

- **Peak Data Rate**

The following definition of Peak Data Rate is from ITU-R M.2410-0 (11/2017) [4]. Peak data rate is the maximum achievable data rate under ideal conditions (in bit/s), which is the received data bits assuming error-free conditions assignable to a single mobile station, when all assignable radio resources for the corresponding link direction are utilised (i.e., excluding radio resources that are used for physical layer synchronisation, reference signals or pilots, guard bands and guard times).

Peak data rate is defined for a single mobile station. In a single band, it is related to the peak spectral efficiency in that band. Let W denote the channel bandwidth and SE_p denote the peak spectral efficiency in that band. Then the user peak data rate R_p is given by Equation 1:

$$R_p = W * SE_p \text{ (eq. 1)}$$

Peak spectral efficiency and available bandwidth may have different values in different frequency ranges. In case bandwidth is aggregated across multiple bands, the peak data rate will be summed over the bands. Therefore, if bandwidth is aggregated across Q bands, then the total peak data rate is:

$$R = \sum_{i=1}^Q W_i * SE_{pi} \text{ (eq.2)}$$

where W_i and SE_{pi} ($i = 1, \dots, Q$) are the component bandwidths and spectral efficiencies respectively.

This requirement is defined for the purpose of evaluation in the eMBB usage scenario.

The minimum requirements for peak data rate are as follows:

- Downlink peak data rate is 20 Gbit/s.
- Uplink peak data rate is 10 Gbit/s

- **User Experienced Data Rate**

The following definition of User Experienced Data Rate is from ITU-R M.2410-0 (11/2017) [4].

User experienced data rate is the 5% point of the cumulative distribution function (CDF) of the user throughput. User throughput (during active time) is defined as the number of correctly received bits, i.e., the number of bits contained in the service data units (SDUs) delivered to Layer 3, over a certain period of time.

In case of one frequency band and one layer of transmission reception points (TRxP), the user experienced data rate could be derived from the 5th percentile user spectral efficiency through equation (3). Let W denote the channel bandwidth and SE_{user} denote the 5th percentile user spectral efficiency. Then the user experienced data rate, R_{user} is given by:

$$R_{user} = W * SE_{user} \text{ (eq.3)}$$

In case bandwidth is aggregated across multiple bands (one or more TRxP layers), the user experienced data rate will be summed over the bands.

This requirement is defined for the purpose of evaluation in the related eMBB test environment.

The target values for the user experienced data rate are as follows in the Dense Urban – eMBB test environment for 5G networks:

- Downlink user experienced data rate is 100 Mbit/s.
- Uplink user experienced data rate is 50 Mbit/s

These values are defined assuming supportable bandwidth as described in Report ITU-R M.2412-0 [8] for each test environment. However, the bandwidth assumption does not form part of the requirement. The conditions for evaluation are described in Report ITU-R M.2412-0 [8].

- **Area Traffic Capacity**

The following definition of Area Traffic Capacity is from ITU-R M.2410-0 (11/2017) [1].

Area traffic capacity is the total traffic throughput served per geographic area (in Mbit/s/m²). The throughput is the number of correctly received bits, i.e., the number of bits contained in the SDUs delivered to Layer 3, over a certain period.

This can be derived for a particular use case (or deployment scenario) of one frequency band and one TRxP layer, based on the achievable average spectral efficiency, network deployment (e.g., TRxP (site) density) and bandwidth.

Let W denote the channel bandwidth and ρ the TRxP density (TRxP/m²). The area traffic capacity area is related to average spectral efficiency SE_{avg} through equation:

$$C_{area} = \rho * W * SE_{avg} \text{ (eq.4)}$$

In case bandwidth is aggregated across multiple bands, the area traffic capacity will be summed over the bands.

This requirement is defined for the purpose of evaluation in the related eMBB test environment.

The target value for Area traffic capacity in downlink is 10 Mbit/s/m² in the Indoor Hotspot – eMBB test environment for 5G networks.

The conditions for evaluation including supportable bandwidth are described in Report ITU-R M.2412-0 [8] for the test environment.

- **Bandwidth**

The following definition of Bandwidth is from ITU-R M.2410-0 (11/2017) [1].

Bandwidth is the maximum aggregated system bandwidth. The bandwidth may be supported by single or multiple radio frequency (RF) carriers. The bandwidth capability of the RIT/SRIT is defined for the purpose of IMT-2020 evaluation.

The requirement for bandwidth is at least 100 MHz.

The RIT/SRIT shall support bandwidths up to 1 GHz for operation in higher frequency bands (e.g., above 6 GHz).

Proponents are encouraged to consider extensions to support operation in wider bandwidths considering the research targets expressed in Recommendation ITU-R M.2083 [6].

The RIT/SRIT shall support scalable bandwidth. Scalable bandwidth is the ability of the candidate RIT/SRIT to operate with different bandwidths.

- **Connection Density**

The following definition of Connection Density is from ITU-R M.2410-0 (11/2017) [4].

Connection density is the total number of devices fulfilling a specific quality of service (QoS) per unit area (per km²).

Connection density should be achieved for a limited bandwidth and number of TRxPs. The target QoS is to support delivery of a message of a certain size within a certain time and with a certain success probability, as specified in Report ITU-R M.2412-0 [8].

This requirement is defined for the purpose of evaluation in the mMTC usage scenario.

The minimum requirement for connection density is 1 000 000 devices per km².

- **Latency**

The following definition of User and Control Plane Latency is from ITU-R M.2410-0 (11/2017) [4].

User Plane Latency: User plane latency is the contribution of the radio network to the time from when the source sends a packet to when the destination receives it (in ms). It is defined as the one-way time it takes to successfully deliver an application layer packet/message from the radio protocol layer 2/3 SDU ingress point to the radio protocol layer 2/3 SDU egress point of the radio interface in either uplink or downlink in the network for a given service in unloaded conditions, assuming the mobile station is in the active state.

This requirement is defined for the purpose of evaluation in the eMBB and URLLC usage scenarios.

The minimum requirements for user plane latency in 5G networks are:

- 4 ms for eMBB
- 1 ms for URLLC

assuming unloaded conditions (i.e., a single user) for small IP packets (e.g., 0 byte payload + IP header), for both downlink and uplink.

Control Plane Latency: Control plane latency refers to the transition time from a most “battery efficient” state (e.g., Idle state) to the start of continuous data transfer (e.g., Active state).

This requirement is defined for the purpose of evaluation in the eMBB and URLLC usage scenarios.

The minimum requirement for control plane latency is 20 ms. Proponents are encouraged to consider lower control plane latency, e.g., 10 ms.

- **Reliability**

The following definition of Reliability is from ITU-R M.2410-0 (11/2017) [4].

Reliability relates to the capability of transmitting a given amount of traffic within a predetermined time duration with high success probability.

Reliability is the success probability of transmitting a layer 2/3 packet within a required maximum time, which is the time it takes to deliver a small data packet from the radio protocol layer 2/3 SDU ingress point to the radio protocol layer 2/3 SDU egress point of the radio interface at a certain channel quality.

This requirement is defined for the purpose of evaluation in the URLLC usage scenario.

The minimum requirement for the reliability is $1-10^{-5}$ success probability of transmitting a layer 2 PDU (protocol data unit) of 32 bytes within 1 ms in channel quality of coverage edge for the Urban Macro-URLLC test environment, assuming small application data (e.g., 20 bytes application data + protocol overhead).

Proponents are encouraged to consider larger packet sizes, e.g., layer 2 PDU size of up to 100 bytes.

- **Peak Spectral Efficiency**

The following definition of Peak Spectral Efficiency is from ITU-R M.2410-0 (11/2017) [4].

Peak spectral efficiency is the maximum data rate under ideal conditions normalised by channel bandwidth (in bit/s/Hz), where the maximum data rate is the received data bits assuming error free conditions assignable to a single mobile station, when all assignable radio resources for the corresponding link direction are utilised (i.e., excluding radio resources that are used for physical layer synchronization, reference signals or pilots, guard bands and guard times).

This requirement is defined for the purpose of evaluation in the eMBB usage scenario.

The minimum requirements for peak spectral efficiencies are as follows:

- Downlink peak spectral efficiency is 30 bit/s/Hz.
- Uplink peak spectral efficiency is 15 bit/s/Hz.

These values were defined assuming an antenna configuration to enable eight spatial layers (streams) in the downlink and four spatial layers (streams) in the uplink. However, this does not form part of the requirement and the conditions for evaluation are described in Report ITU-R M.2412-0 [8].

- **5th Percentile User Spectral Efficiency**

The following definition of 5th Percentile User Spectral Efficiency is from ITU-R M.2410-0 (11/2017) [4].

The 5th percentile user spectral efficiency is the 5% point of the CDF of the normalized user throughput. The normalised user throughput is defined as the number of correctly received bits, i.e., the number of bits contained in the SDUs delivered to Layer 3, over a certain period of time, divided by the channel bandwidth and is measured in bit/s/Hz.

The channel bandwidth for this purpose is defined as the effective bandwidth times the frequency reuse factor, where the effective bandwidth is the operating bandwidth normalised appropriately considering the uplink/downlink ratio.

With $R_i(T_i)$ denoting the number of correctly received bits of user i , T_i the active session time for user i and W the channel bandwidth, the (normalized) user throughput of user i , R_i is defined according to equation 5:

$$R_i = \frac{R_i(T_i)}{T_i(W)} \quad (\text{eq.5})$$

This requirement is defined for the purpose of evaluation in the eMBB usage scenario.

The minimum requirements for 5th percentile user spectral efficiency for various test environments are summarised in the following Table 62.

Table 62: 5th percentile user spectral efficiency.

Test environment	Downlink (bit/s/Hz)	Uplink (bit/s/Hz)
Indoor Hotspot – eMBB0.3	0.3	0.21
Dense Urban – eMBB (NOTE 1)	0.225	0.15
Rural – eMBB	0.12	0.045

NOTE 1 – This requirement will be evaluated under Macro TRxP layer of Dense Urban – eMBB test environment as described in Report ITU-R M.2412-0 [8].

The performance requirement for Rural-eMBB is not applicable to Rural-eMBB LMLC (low mobility large cell) which is one of the evaluation configurations under the Rural- eMBB test environment.

The conditions for evaluation including carrier frequency and antenna configuration are described in Report ITU-R M.2412-0 [8] for each test environment.

- **Average Spectral Efficiency**

The following definition of Average Spectral Efficiency is from ITU-R M.2410-0 (11/2017) [4].

Average spectral efficiency is the aggregate throughput of all users (the number of correctly received bits, i.e., the number of bits contained in the SDUs delivered to Layer 3, over a certain period of time) divided by the channel bandwidth of a specific band divided by the number of TRxPs and is measured in bit/s/Hz/TRxP.

The channel bandwidth for this purpose is defined as the effective bandwidth times the frequency reuse factor, where the effective bandwidth is the operating bandwidth normalized appropriately considering the uplink/downlink ratio.

Let $R_i(T)$ denote the number of correctly received bits by user i (downlink) or from user i (uplink) in a system comprising a user population of N users and M TRxPs. Furthermore, let W denote the channel bandwidth and T the time over which the data bits are received. The average spectral efficiency, SE_{avg} is then defined according to equation 6:

$$SE_{avg} = \sum_{i=1}^N \frac{R_i(T)}{T * W * M} \quad (\text{eq.6})$$

This requirement is defined for the purpose of evaluation in the eMBB usage scenario.

The minimum requirements for average spectral efficiency for various test environments are summarized in Table 63.

Table 63: Average spectral efficiency.

Test environment	Downlink (bit/s/Hz)	Uplink (bit/s/Hz)
Indoor Hotspot – eMBB0.3	0.3	0.21
Dense Urban – eMBB (NOTE 1)	0.225	0.15
Rural – eMBB	0.12	0.045

NOTE 1 – This requirement applies to Macro TRxP layer of the Dense Urban – eMBB test environment as described in Report ITU-R M.2412-00 [8].

The performance requirement for Rural-eMBB is also applicable to Rural-eMBB LMLC which is one of the evaluation configurations under the Rural- eMBB test environment. The details (e.g. 8 km inter-site distance) can be found in Report ITU R M.2412-0 [8].

The conditions for evaluation including carrier frequency and antenna configuration are described in Report ITU-R M.2412-0 [8] for each test environment.

- **Energy Efficiency**

The following definition of Energy Efficiency is from ITU-R M.2410-0 (11/2017) [4].

Network energy efficiency is the capability of a RIT/SRIT to minimize the radio access network energy consumption in relation to the traffic capacity provided. Device energy efficiency is the capability of the RIT/SRIT to minimize the power consumed by the device modem in relation to the traffic characteristics.

Energy efficiency of the network and the device can relate to the support for the following two aspects:

- Efficient data transmission in a loaded case.
- Low energy consumption when there is no data.

Efficient data transmission in a loaded case is demonstrated by the average spectral efficiency.

Low energy consumption when there is no data can be estimated by the sleep ratio. The sleep ratio is the fraction of unoccupied time resources (for the network) or sleeping time (for the device) in a period corresponding to the cycle of the control signalling (for the network) or the cycle of discontinuous reception (for the device) when no user data transfer takes place. Furthermore, the sleep duration, i.e., the continuous period of time with no transmission (for network and device) and reception (for the device), should be sufficiently long.

This requirement is defined for the purpose of evaluation in the eMBB usage scenario.

The RIT/SRIT shall have the capability to support a high sleep ratio and long sleep duration. Proponents are encouraged to describe other mechanisms of the RIT/SRIT that improve the support of energy efficient operation for both network and device.

- **Energy Efficiency in NFV**

The following definition of Energy Efficiency in NFV is from ETSI EN 303 471 V1.1.1 (2019- 01) [9] and the metric is defined in 3GPP TS 22.261 V16.4.0 (2018-06) [10].

Energy efficiency in NFV is calculated based on data transfer (KPIEE-transfer). The document specifies two variants of KPIEE-transfer (KPIEE-bit transfer and KPIEE-packet transfer) which are measures of the data volume transferred to and from the NFVI per unit of energy consumed by the NFVI as shown schematically in the following figure.

The determination of the effectiveness of such NFVI in effecting a reduction of energy consumption depend upon knowledge of the energy consumption of the NFVI and data volume transmitted and received by the NTE with the NFVI.

KPIEE-bit transfer is based on the data volume defined by the arithmetic sum of Layer 2 payload content of the number of successfully transmitted and received bits. KPIEE-packet transfer is based on the data volume defined by the arithmetic sum of successfully transmitted and received packets.

KPIEE-bit transfer and KPIEE-packet transfer do not take account of:

- the energy consumption involved in the transport of the data to and from the NFVI beyond the physical interface;
- the energy consumption of any processing of the data (e.g., routing, etc.) beyond the physical interface .

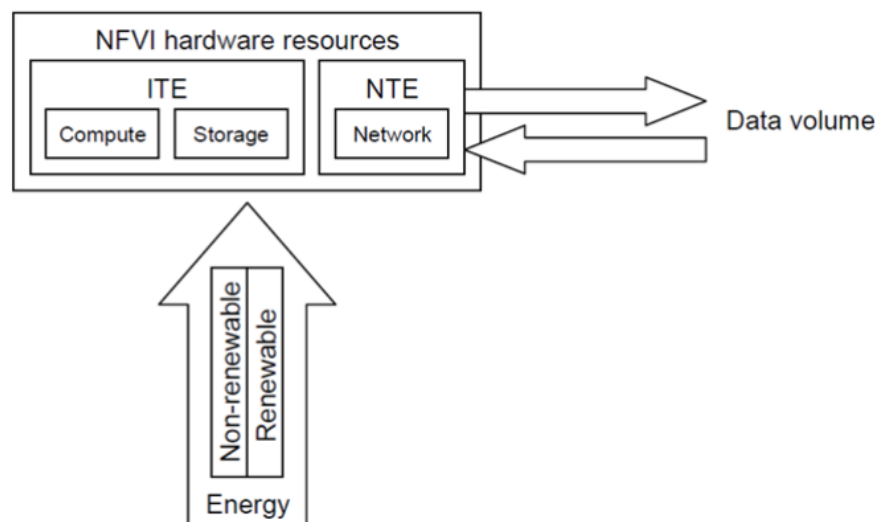


Figure 36: Energy efficiency in NFV on data transfer [9].

- **Higher-Accuracy Positioning**

The following definition of Higher-Accuracy Positioning in NFV is from 3GPP TS 22.261 V16.4.0 (2018-06) [10].

Higher accuracy positioning is characterized by ambitious system requirements for positioning accuracy. One typical area where “higher-accuracy positioning” is needed is collision avoidance of vehicles: every vehicle must be aware of its own position, the positions of near-by vehicles, and their expected paths, to avoid collisions. On the factory floor, it is important to locate moving objects such as forklifts, or parts to be assembled.

The 5G system shall support the use of 3GPP and non-3GPP technologies to achieve higher accuracy positioning.

The corresponding positioning information shall be acquired in a timely fashion, be reliable, and be available (e.g., it is possible to determine the position).

UEs shall be able to share positioning information between each other e.g., to a controller if the location information cannot be processed or used locally.

For mobile objects on factory floor, 3GPP TS 22.261 [10] defines:

- Position acquisition time: 500 ms
- Survival time: 1 s
- Availability: 99.99%
- Dimension of service area: 500x500x30m
- Position accuracy: 0.5 m

- **Quality of Experience**

The Quality of experience (QoE) has been defined by the ITU-T Recommendation P.10/G.100 (ITU-T 2017) [11] as “the overall acceptability of an application or service, as perceived subjectively by the end-user”, covering the complete end-to-end system effects (client, terminal, network, services infrastructure, etc.). Hence, the QoE is subjective by definition, because of its relationship with user’s viewpoint, expectations, and context. Hence, since measuring a subjective QoE may differ from one client to another, it is usually estimated using objective parameters. For example, the most popular objective video quality estimation methods are Human and nonhuman Visual System (HVS) perception, covering QoS parameters, such as peak SNR, Video Quality Model (VQM), Perceptual Video Quality of Experience (PEVQ), Perceptual Quality Index (PQI), etc.

The ability to measure QoE would provide network operators with some sense of the contribution of the network’s performance to the overall customer satisfaction, in terms of reliability, availability, scalability, speed, accuracy and efficiency. The factors that affect the user perceived QoE are bandwidth, jitter, delay, and packet loss rate. The mean opinion score (MOS) is an example of a subjective measurement method in which users rate the service quality by giving five different point scores, from 5 to 1, where 5 is the best quality and 1 is the worst quality. Quality can be classified as Bad [0 – 1], Poor [1 – 2], Fair [2 – 3], Good [3 – 4] and Excellent [4 – 5]. The minimum requirement is to have MOS values > 4.3.

The Hexa-X⁷² project identified the following KPI, some are based on KVM WG:

- **Data rate:** Peak data rates.
- **Capacity:** the total traffic capacity per area.
- **Localization:** Precision and accuracy in positioning services.
- **Connection density:** The number of served/connected devices in an area.
- **Service availability:** the fraction of device population for which a service can be delivered with a certain availability; minimum service interruption due to events or mobility; and network survivability over time.
- **Deterministic services:** deliver guarantees for: achievable data rate; maximum end-to-end service latency; and end-to-end packet reliability in order to enable, e.g., use cases from the automation domain or in human-machine interaction.
- **Coverage:** fraction of global surface covered; fraction of population, covered; total cost of coverage per area; and traffic volume while providing 6G performance and services.
- **Integrated sensing:** The intrinsic properties of localization and sensing rely on traditional sensing parameters such as relative precision in position and velocity; angular resolution; accuracy in parameter estimation; and

⁷² Hexa-X project deliverable D1.2: https://hexa-x.eu/wp-content/uploads/2021/05/Hexa-X_D1.2.pdf

convergence time of estimation. However, the system co-design for both, communications, and sensing purposes, allows for enhanced performance in terms of coverage and throughput, as well as service interruption during mobility.

- **Local compute integration:** The intrinsic properties of local compute integration will be key parameters such as RTT to compute and storage as well as time-to-market to introduce additional compute capabilities. However, the integration of local compute capabilities is done to enhance other features which could be measured with use-case specific KPIs, for example, Quality of Immersion.
- **Integrated intelligence:** Integration of AI/ML encompasses both utilization of AI/ML for optimization of network operations in a pervasive way (for example, AI/ML-defined air interface framework), as well as

optimisation of network operations for optimal performance of AI/ML features. For the utilisation of AI/ML to enhance network features, the relevant parameters will be e.g., convergence time; enhancements over existing analytical or heuristic features; fault rate; and added energy consumption. For the optimization of the network to facilitate AI/ML features, the relevant parameters will rather be flexibility to adjust parameters; time-to-market of new features.

- **Embedded devices:** If a wireless device is to be embeddable anywhere, access to an external power source cannot be taken for granted. In addition, the placement of the devices may prevent or prohibit the usage of batteries as a power source. Therefore, these devices may rely on energy-harvesting of some form and to keep down cost, the devices may be produced using printable electronics.

Key aspects to consider for embeddable devices are energy consumption; form factor; cost; time

between maintenance occasions; total resource consumption and end-of-life handling.