



SAFE-6G

A Smart and Adaptive Framework for Enhancing Trust in 6G Networks

Deliverable D6.4: Standardization, Innovation, Exploitation and Technology Transfer Activities (Intermediate)

Date: 30/06/2025

Version: V1.0

DISCLAIMER

This document contains information, which is proprietary to the SAFE-6G (“A Smart and Adaptive Framework for Enhancing Trust in 6G Networks”) Consortium that is subject to the rights and obligations and to the terms and conditions applicable to the Grant Agreement number: 101139031. The action of the SAFE-6G Consortium is funded by the European Commission.

Neither this document nor the information contained herein shall be used, copied, duplicated, reproduced, modified, or communicated by any means to any third party, in whole or in parts, except with prior written consent of the SAFE-6G Consortium. In such case, an acknowledgement of the authors of the document and all applicable portions of the copyright notice must be clearly referenced. In the event of infringement, the consortium reserves the right to take any legal action it deems appropriate.

This document reflects only the authors’ view and does not necessarily reflect the view of the European Commission. Neither the SAFE-6G Consortium as a whole, nor a certain party of the SAFE-6G Consortium warrant that the information contained in this document is suitable for use, nor that the use of the information is accurate or free from risk, and accepts no liability for loss or damage suffered by any person using this information.

The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Grant Agreement	101139031
Document number	D6.4
Document title	Standardisation, Innovation, Exploitation and Technology Transfer Activities (Intermediate)
Lead Beneficiary	THALES
Editor(s)	Stephane Lorin, Pascal Bisson (THA)
Author(s)	Nikolaos Zombakis (8BELLS) Vasilis Mavrikakis (INF) Javier Garcia Rodrigo (TID) Vaios Koumaras (INF) Alejandro Fornés (UPV) Victoria Katsarou (SHG) Marios Sofophocleous (EBOS) Dimitris Zouzias (EBOS) Christos Xenakis (IQBT) Kushlal Mehta (IQBT) Raisia Gorbunov (IQBT) Harilaos Koumaras (NCSR D) Spyridon Georgoulas (NCSR D) Vasiliki Rentoula (NCSR D) Efi Markoulaki (NCSR D) And all partners in task 6.4 (individual exploitation plans)
Dissemination level	Public
Contractual date of delivery	30/06/2025
Status	Final
File name	SAFE-6G_D6.4_v1.0.doc

Revision History

Version	
V0.1	Table of Contents.
V0.2	Exploitation contributions.
V0.3	Standardization contributions.
V0.4	First internal review done by ATOS and TID.
V0.5	Version produced by THA based on the comments from the First Review. Second review performed by the Technical Steering Committee.
V0.6	Final draft and homogenization of content produced by THA. Final review performed by the Project Coordinator and the Editor.
V1.0	Final version following the Quality check.

GLOSSARY

Abbreviations/Acronym	Description
3GPP	Third Generation Partnership Project
AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
BDS	Big Data & Security
CA	Consortium Agreement
CAGR	Compound Annual Growth Rat
CAPIF	Common API Framework
DL	Deep Learning
dLoR	Desired Level of Resilience
DoA	Document of Action
DP	Differential Privacy
DT	Digital Twin
E2E	End to End
EC	European Commission
EDF	European Defence Fund
ENI	Experiential Network Intelligence
ENISA	European Union Agency for Cybersecurit
ETSI	European Telecommunications Standards Institute
EU	European Union
FG	Focus Group
GA	Grant Agreement
HPC	High-performance computing
ICT	Information and Communication Technologies
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IP	Intellectual Property
IPR	Intellectual Property Rights
ISG	Industry Specification Group
ITU-T	International Telecommunication Union Telecommunication
JEPs	Joint Exploitation Plans
JU	Joint Undertaking
KPI	Key Performance Indicator
LLMs	Large Language Models
LoR	Level of Resilience
LoT	Level of Trust
LoTw	Level of Trustworthiness
LSP	Large-Scale Partnership
ML	Machine Learning
MLOps	Machine Learning Operations
NFV	Network Functions Virtualisation
NGMN	Next Generation Mobile Networks
NIST	National Institute of Standards and Technology
nLoT	non-calibrated Level of Trustworthiness
NLP	Natural Language Processing
ProSe	Proximity Services

QoD	Quality on Demand
QoS	Quality of Service
R&D	Research and Development
SACM	Security Automation and Continuous Monitoring
SAI	Securing Artificial Intelligence
SBA	Service Based Architecture
SDG OCF	Software Development Group Open CAPIF
SDN	Software Defined Networking
SDO	Standard Developing Organization
SDPs	Software-Defined Perimeters
SDQC	Software-Defined Quantum Communication
SI	Study Items
SNS	Smart Networks and Services
SSI	Self-Sovereign Identity
TAM	Total Addressable Market
TC	Technical Committee
TM	Technical Manager
TSG SA	Technical Specification Group Service and System Aspects
VCs	Verifiable Credentials
VNFs	Virtual Network Functions
VR	Virtual Reality
W3C	World Wide Web Consortium
WG	Working Group
WI	Work Items
XAI	eXplainable AI
XR	Extended Reality

EXECUTIVE SUMMARY

This document is in the continuation of deliverable D6.2, which described initial plans and roadmaps for the standardisation (task 6.3) and innovation and exploitation of the results of the project (task 6.4) developed in the SAFE-6G project. This deliverable provides an update on the progress made.

Regarding standardisation, this intermediate deliverable presents the initial results based on the ongoing exchanges with four SDOs and relevant initiatives that partners have engaged with them: 3GPP, ETSI, CAMARA and ENISA.

Regarding innovation and exploitation, the deliverable presents an initial outline of the individual exploitation plans developed by partners and identifies the list of technology assets that the project is developing. These assets have then been scored and ranked across multiple dimensions—such as technological maturity, commercial potential, strategic fit and ecosystem impact. With these scores, the goal is to ensure that each innovation is not only technically relevant but also positioned for successful deployment and adoption within the broader 6G landscape. Another goal is to build also a composite score to offer a holistic view of the result's overall exploitation potential. Lastly, works to build joint exploitation plans have been initiated.

This deliverable will be followed in M36 by the final results of the works done in tasks 6.3 and 6.4 and reported in deliverable *D6.6: Standardisation, Innovation, Exploitation and Technology Transfer Activities (Final)*.

KEYWORDS

Standardization, Innovation, Exploitation plan, IPR, SDO, 6G

TABLE OF CONTENTS

1	<i>Introduction</i>	1
1.1	Document objective.....	1
1.2	Document Structure	1
2	<i>Standardization</i>	2
2.1	Introduction	2
2.2	Refinement of types of contributions	2
2.3	Works with SDOs and relevant initiatives	3
2.3.1	Introduction	3
2.3.2	3GPP – SA 1, 3 & 6.....	3
2.3.3	ETSI – SDG OCP (Software Development Group Open CAPIF)	8
2.3.4	ETSI – SAI.....	10
2.3.5	CAMARA – Quality on Demand (QoD)	11
2.3.6	ENISA – Emerging Technologies.....	11
2.4	Conclusion and next steps.....	12
2.4.1	Engaged works	12
2.4.2	Next steps.....	13
2.4.3	New opportunities	13
2.4.4	Follow-up.....	13
3	<i>Exploitation Plans and IPR management</i>	14
3.1	Introduction	14
3.2	IP Rights (IPR) management approach.....	15
3.3	Individual exploitation plans	16
3.3.1	Introduction	16
3.3.2	Telefonica Exploitation Plan.....	16
3.3.3	NCSR D Exploitation Plan	20
3.3.4	THALES Exploitation Plan	23
3.3.5	INQBIT Exploitation Plan	26
3.3.6	EVIDEN Exploitation Plan	32
3.3.7	UNIWA Exploitation Plan.....	43
3.3.8	SPACE HELLAS Exploitation Plan	46
3.3.9	INFOLYSIS Exploitation Plan	50
3.3.10	EBOS Exploitation Plan	55
3.3.11	UPV Exploitation Plan	62
3.3.12	8BELLS Exploitation Plan.....	68
3.3.13	CUMUCORE OY Exploitation Plan.....	73
3.3.14	IMMERSION Exploitation Plan	77

3.4	Evaluation of Key Exploitable Results	88
3.4.1	Top-Ranked Exploitable Results -Key exploitable results	91
3.4.2	Insights and Next Steps	93
3.5	Joint Exploitation.....	93
3.5.1	Joint Exploitation Plan 1 – SAFE-6G Use Case 1: Industrial Metaverse of a Production Line	94
3.5.2	Joint Exploitation Plan – SAFE-6G Use Case 2: Metaverse for education.....	105
3.6	Conclusion & Next Steps	122
4	Conclusion.....	124
5	References	125

List of FIGURES

Figure 1: Standardization tab in EC portal 2
 Figure 2: Timeframe for Release 19..... 5
 Figure 3: Timeframe for Release 19..... 5
 Figure 4: Screenshot of openCAPIF ecosystem for SAFE-6G 9
 Figure 5: Eviden Big Data & Security department 35
 Figure 6: Global Private 5G Network Market Forecast 76
 Figure 7: SAFE-6G Product RoadMap - Gantt Chart..... 84

List of TABLES

Table 1: Types of contributions and actions towards SDOs and relevant initiatives..... 3
 Table 2: 3GGP SA6 contributions related to OpenCAPIF 8
 Table 3: Engaged works with SDOs and relevant initiatives 12
 Table 4: Next steps for already engaged works with SDOs/relevant initiatives..... 13
 Table 5: Summary of Exploitable Results (Telefonica)..... 20
 Table 6: Summary of Exploitable Results (NCSR) 23
 Table 7: Summary of Exploitable Results (Thales) 25
 Table 8: Summary of Exploitable Results (INQBIT) 32
 Table 9: MLOPs challenges and reported solutions (from literature) 39
 Table 10: Summary of Exploitable Results (Eviden)..... 43
 Table 11: Summary of Exploitable Results (UNIWA) 46
 Table 12: Summary of Exploitable Results (SPACE) 50
 Table 13: Summary of Exploitable Results (INFOLYSIS) 55
 Table 14: Summary of Exploitable Results (eBOS)..... 61
 Table 15: Summary of Exploitable Results (UPV)..... 68
 Table 16: Summary of Exploitable Results (8BELLS) 73
 Table 17: Summary of Exploitable Results (CUMUCORE) 77
 Table 18: Summary of Exploitable Results (IMM)..... 88
 Table 19: Exploitable Results Evaluation 91
 Table 20: SAFE-6G Technology–Capability Alignment 121

1 INTRODUCTION

1.1 DOCUMENT OBJECTIVE

The SAFE-6G project focuses on developing a novel architecture and a suite of components aimed at providing trustworthiness in user-centric distributed 6G systems. The goal is to propose native trustworthiness, clarifying that the term "trustworthiness" refers to a holistic approach, including safety, security, privacy, resilience and reliability. Moreover, a realistic solution to this trustworthiness challenge must recognize that all security measures (i.e., safety, security, privacy, resilience and reliability) come at a cost in terms of usability, agility, or swiftness. As a result, the envisioned trustworthiness framework should provide a balance between the various security measures by dealing with a security-by-design approach, as well as a wide range of themes, such as the trust model and the application of new cognitive coordination technologies (e.g., Intent-based trustworthiness, Artificial Intelligence (AI) and Machine Learning (ML) techniques).

Deliverable [*D6.2- Standardisation, Innovation, Exploitation and Technology Transfer Plan*](#), published in month 8 (M8) presented the initial plans for aligning to Standard Developing Organizations (SDOs) that are most relevant to the project and contributing the main project results to them (task 6.3). The deliverable also presented initial plans to ensure a commercial exploitation and impact assessment of project results (task 6.4).

This document covers the first results of the implementation of these initial plans. This document will be followed by a final version of *D6.6-Standardisation, Innovation, Exploitation and Technology Transfer Activities (Final)* due by the end of the project, document that will present the final results of the implementation of these plans.

1.2 DOCUMENT STRUCTURE

Besides this introductory chapter, the structure of this document is as follows:

- Chapter 2 presents the first actions that have done regarding standardization activities. These actions concern the interactions with four of the SDOs and relevant initiatives that have been identified as the most pertinent for the project: 3GPP, ETSI, CAMARA and ENISA.
- Chapter 3 presents the individual exploitation plans agreed exploitation strategy methodology and roadmap regarding exploitation and innovation plans.
- Chapter 4, Conclusion, presents a summary of the work done and the next steps.

2 STANDARDIZATION

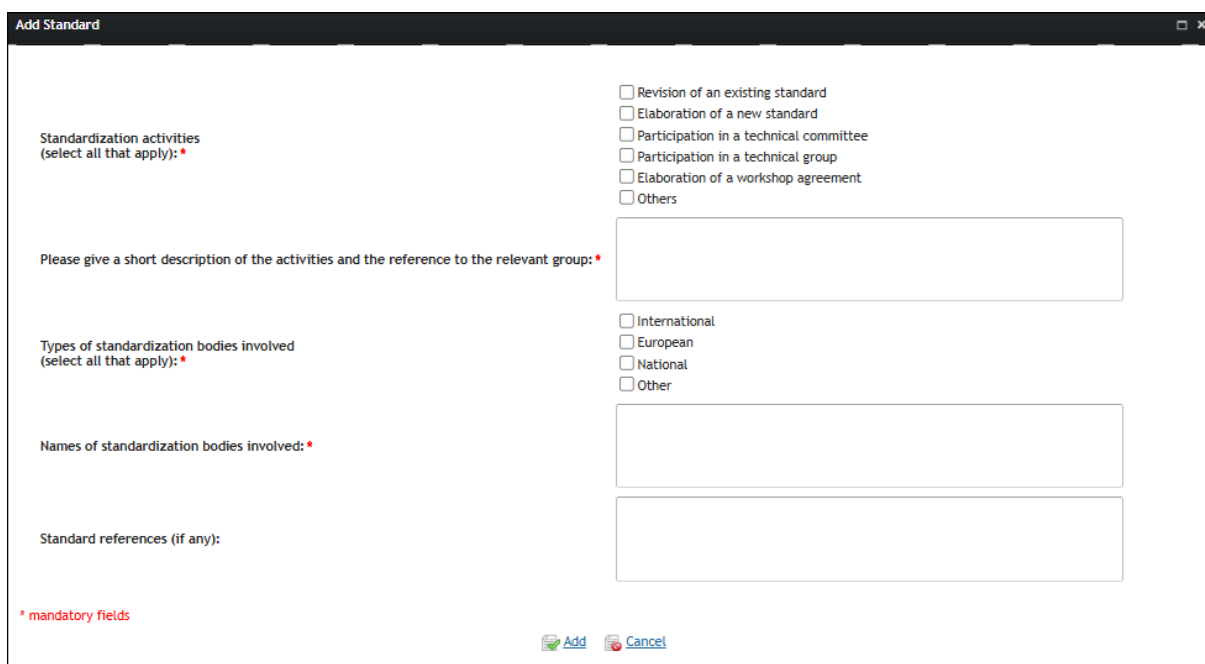
2.1 INTRODUCTION

The deliverable [D6.2](#) presented the initial plan for standardization activities in the context of SAFE-6G project. The initial plan targeted key SDOs for SAFE-6G and defined different types of contribution to address them (from activity monitoring of these organizations until work item proposition for potential integration into a new/existing standard).

Based on this plan, the project has engaged works with the most promising SDOs and working groups related to SAFE-6G, as described in Section 2.3.

2.2 REFINEMENT OF TYPES OF CONTRIBUTIONS

To ease the integration of the results within the European Commission (EC) portal, SAFE-6G crossed the types of contribution defined in deliverable D6.2 with the types of contribution defined in the EC portal (see Figure 1 below):



The screenshot shows a web form titled "Add Standard" with the following fields and options:

- Standardization activities (select all that apply):***
 - Revision of an existing standard
 - Elaboration of a new standard
 - Participation in a technical committee
 - Participation in a technical group
 - Elaboration of a workshop agreement
 - Others
- Please give a short description of the activities and the reference to the relevant group:*** (Text input field)
- Types of standardization bodies involved (select all that apply):***
 - International
 - European
 - National
 - Other
- Names of standardization bodies involved:*** (Text input field)
- Standard references (if any):** (Text input field)

At the bottom left, there is a red asterisk legend: *** mandatory fields**. At the bottom center, there are "Add" and "Cancel" buttons.

Figure 1: Standardization tab in EC portal

These new EC portal suggestions aim at identifying pertinent actions towards SDOs and relevant initiatives. Based on that and on the first actions we engaged with SDOs and relevant initiatives, we refined the types of contribution based on three fundamental pillars:

- **Monitoring and Information Gathering:** Monitoring activities within each SDO or initiative will keep us informed and ensure our contributions are relevant and timely.
- **Active Engagement and Collaboration:** Active participation in meetings and workshops will allow us to present our research findings and proposed standards effectively. Engaging

representatives from SDOs in SAFE-6G meetings will foster collaboration and alignment with ongoing efforts.

- **Contributing and Influencing Standardization:** Proposing new study and work items that may lead to new standards based on SAFE-6G results, such as components, architectures, and methodologies, will ensure our innovations are integrated into the broader standardization landscape.

Results are displayed in Table 1 below.

<i>EC standardization groups</i>	<i>Revision of existing standard</i>	<i>Elaboration of a new standard</i>	<i>Participation in a technical committee</i>	<i>Participation in a technical group</i>	<i>Elaboration of a workshop agreement</i>	<i>Other</i>
Monitoring activity						x
Active engagement			x	x	x	
Contributing and influencing standardization	x	x	x	x	x	

Table 1: Types of contributions and actions towards SDOs and relevant initiatives

2.3 WORKS WITH SDOs AND RELEVANT INITIATIVES

2.3.1 INTRODUCTION

Following a thorough analysis of the standardization landscape in D6.2, the SAFE-6G project has prioritized the following SDOs and associated initiatives relevant to the technical scope of the project. Following axes have guided the selection of these SDOs and relevant initiatives: active involvement of partners with SDOs and key technical aspects for the project (security of 5G/6G, security of Artificial Intelligence AI, API development guidelines, open and secure API exposure, trustworthiness of 6G).

This section is dedicated to report all activities related to the contributions and interactions between the SDOs and the SAFE-6G project itself.

2.3.2 3GPP – SA 1, 3 & 6

2.3.2.1 SCOPE

3GPP offers different Technical Specification Group Service and System Aspects (TSG SA). In particular, the groups SA 1 and v 3 has been identified as very pertinent for SAFE-6G project:

- SA1: SA1 is responsible for defining use cases and service-level requirements. For Release 19, priority topics include enabling applications such as the metaverse and mission-critical services. This group is currently finalizing Stage 1 studies and preparing to move into Stage 2.
- SA3 (Security and Privacy): SA3 focuses on refining security protocols to support advanced 5G applications, particularly scenarios involving indirect network sharing and critical communications.
- SA6 (Application Enablement): Key innovations under SA6 include:

- Mission-Critical Services: Enhancements to improve reliability for critical applications.
- IoT Messaging: Strengthened support for large-scale IoT deployments.
- Localized Applications: Initiatives to enable edge-based extended reality (XR) and metaverse experiences.

2.3.2.2 ENGAGED WORKS

Regarding 3GPP, it is important to provide a temporal context for the framework, especially in relation to all activities connected to 6G. While Release 19 (Rel-19) focuses on maturing and expanding 5G technologies and preparing security and AI frameworks, Rel-20 aims to establish the foundational standards for 6G, introducing transformative capabilities that go beyond 5G-Advanced.

Indeed, 3GPP Rel-19 represents the next step in the evolution of 5G-Advanced, building upon the foundations of previous releases to enhance system performance, support new use cases, and prepare for the eventual transition to 6G. Its objectives include:

- **Enhancing Network Capabilities:** Rel-19 seeks to optimize Quality of Service (QoS), improve energy efficiency, and extend the support for emerging technologies like XR, AI/ML, and industrial automation.
- **Supporting New Applications:** From localized mobile metaverse experiences to advanced IoT and critical communication services, Rel-19 aims to expand the 5G ecosystem.
- **Sustainability and Scalability:** The release emphasizes sustainable network operation and the ability to scale for future demands

In contrast, Rel-20 is widely anticipated to represent the first formal step into 6G standardisation within 3GPP. Its scope is expected to encompass a comprehensive set of novel technologies and paradigms that define 6G, including:

- Native AI/ML-driven network intelligence and zero-trust security architectures, enabling autonomous, trustworthy, and resilient network operations.
- Advanced integration of edge and cloud computing, supporting ultra-reliable, low-latency communications for emerging applications such as Digital Twins (DTs) and XR.
- Utilization of new spectrum bands beyond 5G frequencies (e.g., sub-THz ranges), aligned closely with the ITU-R IMT-2030 framework to translate the 6G vision into concrete technical specifications.

3GPP Release 19 (Rel-19) is expected to be finalized at the end of 2025, focusing on advancing 5G-Advanced features and preparing the groundwork for 6G capabilities. Meanwhile, Release 20 (Rel-20) started in early 2025 and is expected to be completed around 2026 to 2027, marking the first formal step toward 6G standardization within 3GPP. The timeframe of the Release 19 is displayed in Figure 2 and the timeframe of the Release 20 in Figure 3.

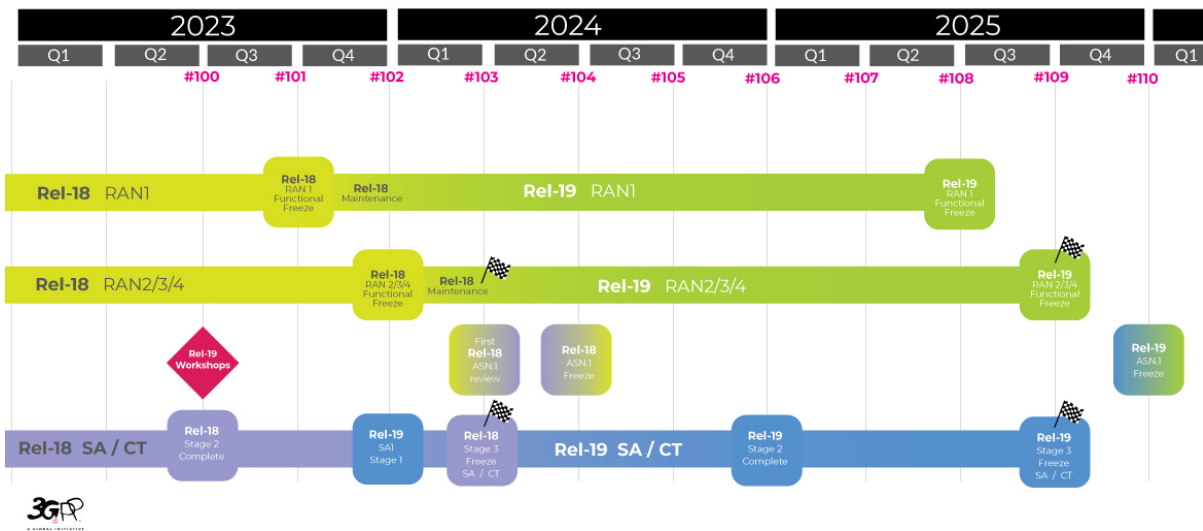


Figure 2: Timeframe for Release 19

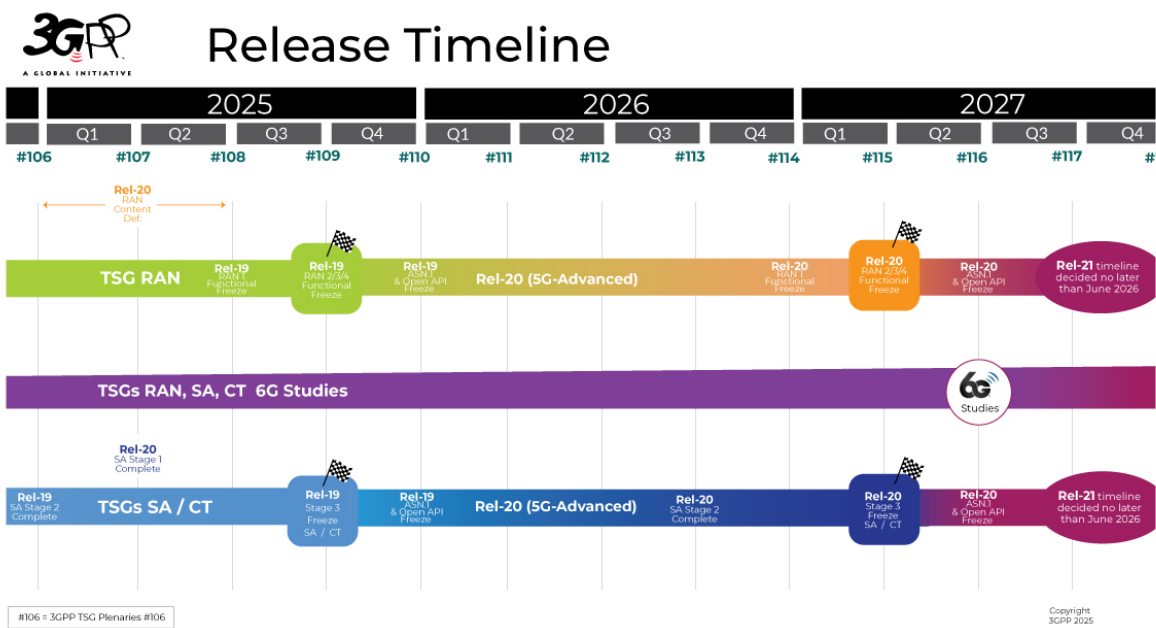


Figure 3: Timeframe for Release 19

Based on the three previously identified categories and the type of activities the project is undertaking in relation to SDOs, the following contributions are identified for 3GPP:

3GPP SA1 and SA3: So far, most of the work has focused on actively monitoring the various **Study Items (SI)** and **Work Items (WI)** currently under discussion within each working group. Of relevance to SAFE-6G are:

- **SA1 (Rel-20) Mission-Critical Services.** Study Item: *FS_MCS_Ext_Arch*
This item addresses the evolution of mission-critical service architecture, including

enhancements for interoperability, off-network operation, and support for non-terrestrial networks (NTNs). This aligns closely with SAFE-6G’s focus on **reliable and resilient communication systems** supporting critical verticals.

- **SA3**

(Rel-19) Proximity Services (ProSe) Security- Study Item: *FS_ProSe_Sec_Enh*
A new study was initiated to evaluate and enhance security mechanisms for multi-hop relaying in ProSe, particularly for UE-to-Network (MU2N) and UE-to-UE (MU2U) communications. These enhancements are crucial for ensuring **trust and integrity** in device-to-device and ad hoc networking scenarios.

(Rel-20) AI/ML Security – Expected Study Item under 6G security evolution (tentative: *FS_AI_Sec*) SA3 is expected to explore **security and privacy challenges** associated with the integration of AI/ML technologies in mobile networks. This includes threat modelling, mitigation strategies, and trust frameworks, which are directly relevant to SAFE-6G’s objectives on privacy-aware AI-driven networking.

- **SA6**

SAFE-6G has been actively following the activities of 3GPP SA6, the group responsible for the specification of application-layer functional architectures and service enablers. As a result of the work being carried out within ETSI and the Open Common API Framework (OpenCAPIF) SDG, the following contributions related to 3GPP SA6 on CAPIF guidelines have been made and are described in Table 2:

Target Study Item/Work Item	Meeting Name	Meeting Date	Type Of Contribution	Area of Work Programme	Impact Achieved
TR 23.946 Rel 19 (version 0.3.0)	TSGS6_060_Changes	apr-24	Technology/Solution;	8. System Architecture	S6-240529 Open source implementation of CAPIF for TR 23.946
TR 23.946 Rel 19 (version 0.6.0)	TSGS6_062_Maastricht	aug-24	Technology/Solution;	8. System Architecture	S6-243631: Accepted contributions to TR 23.946 on OpenCAPIF example for NEF API Exposure using OpenCAPIF (section 6.4 NEF Publishes an API)
TR 23.946 Rel 19 (version 0.6.0)	TSGS6_062_Maastricht	aug-24	Technology/Solution;	8. System Architecture	S6-243633: Accepted contributions to TR 23.946 on OpenCAPIF example for API Invoker using OpenCAPIF (section 6.8 API consumption from an API Invoker)
TR 23.946 Rel 19 (version 0.6.0)	TSGS6_062_Maastricht	aug-24	Technology/Solution;	8. System Architecture	S6-243510: Accepted contributions to TR 23.946 on OpenCAPIF examples using

					POSTMAN for examples in the document (Annex A: Examples from OpenCAPIF).
TR 23.946 Rel 19 (version 0.6.0)	TSGS6_062_Maastricht	aug-24	Technology/Solution;	8. System Architecture	S6-243265: Update and alignment of the listed APIs that OpenCAPIF has adopted from CAPIF with the terminology used in 3GPP TS 29.222.
TR 23.946 Rel 19	TSGS6_063_India	oct-24	Technology/Solution;	8. System Architecture	S6-244198: ETSI MEC deployment based on CAPIF
TR 23.946 Rel 19	TSGS6_063_India	oct-24	Technology/Solution;	8. System Architecture	S6-244557: NEF AEF profile updates
TR 23.946 Rel 19	TSGS6_063_India	oct-24	Technology/Solution;	8. System Architecture	S6-244558: pCR on Supported Features
TR 23.946 Rel 19	TSGS6_063_India	oct-24	Technology/Solution;	8. System Architecture	S6-244559: CAPIF Core Function APIs test Annex
TR 23.946 Rel 19	TSGS6_064_Orlando	nov-24	Technology/Solution;	8. System Architecture	S6-245430 CAPIF Vendor Extensibility
TR 23.946 Rel 19	TSGS6_064_Orlando	nov-24	Technology/Solution;	8. System Architecture	S6-245431 MEC Platform as an API Provider
TR 23.946 Rel 19 (version 1.0.0) Publication	TSGS6_064_Orlando	nov-24	Technology/Solution;	8. System Architecture	TR 23.946 first publication as part of Release 19
TR 23.946	TSGS6_065_Athens	feb-25	Technology/Solution;	8. System Architecture	S6-250365 Correction to obtaining CAPIF credentials
AI/ML Service Enablement	TSGS6_065_Athens	feb-25	Technology/Solution;	8. System Architecture	S6-250559 New SID on application enablement for AI/ML service; Phase 2
TR 23.946	TSGS6_066_Gothenburg	apr-25	Technology/Solution;	8. System Architecture	S6-251128 CAPIF_EXT Authentication and Authorization info
TR 23.946	TSGS6_066_Gothenburg	apr-25	Technology/Solution;	8. System Architecture	S6-251165 CAPIF_EXT Annex C errors and omissions
External TR 23.XXX	TSGS6_067_Fukuoka	apr-25	Technology/Solution;	8. System Architecture	S6-252547 New WID on Guidelines for Application Enablement usage

Internal 23.XXX	TR	TSGS6_067_Fuku oka	apr-25	Technology/ Solution;	8. System Architect ure	S6-252541 New study item on CAPIF Phase 4
----------------------------	-----------	-----------------------	--------	--------------------------	-------------------------------	--

Table 2: 3GPP SA6 contributions related to OpenCAPIF

2.3.2.3 NEXT STEPS

As 3GPP progresses toward the finalization of Release 19 by the end of 2025 and enters the formative stages of Release 20, the SAFE-6G project will continue to align its activities with key standardization topics. In the short term, efforts will focus on reinforcing monitoring and targeted contributions to Study Items within SA1 and SA3, particularly those related to mission-critical services, Proximity Services (ProSe) security, and the emerging AI/ML security landscape. These areas are directly aligned with SAFE-6G’s objectives on resilient, trustworthy, and intelligent communication systems. Additionally, SAFE-6G will build upon its early contributions to 3GPP SA6 by continuing its engagement in CAPIF-related discussions, ensuring that European perspectives are well represented in the evolution of service enablers and API frameworks.

Looking ahead, the project will strategically plan for potential contributions to Release 20, especially on topics such as native AI/ML integration, zero-trust architectures, and support for critical 6G verticals. Collaboration with ETSI, OpenCAPIF, and other relevant SDOs will be key to shaping a coherent and forward-looking European input into 6G standardization.

2.3.3 ETSI – SDG OCP (SOFTWARE DEVELOPMENT GROUP OPEN CAPIF)

2.3.3.1 SCOPE

The Software Development Group Open CAPIF (SDG OCF) is developing an open-source Common API Frameworks, as described by 3GPP, allowing to expose and consume APIs in a secure and consistent way. OpenCAPIF can handle:

- Publication of APIs by network or service providers.
- Discovery and consumption of APIs by authorized consumers, Secure onboarding and access control of client and providers of APIs.
- Logging and monitoring.

ETSI SDG OCF collaborates with other ETSI software and open-source projects, such as Open-Source MANO, TeraFlowSDN and OpenSlice, in order to share best practices and find synergies, joint activities, and opportunities for component reuse.

2.3.3.2 ENGAGED WORKS

SAFE-6G is actively engaged in the Open CAPIF ecosystem and contributes to the ongoing development of CAPIF specifications. One of the core objectives is to identify and develop new APIs (either as providers or invokers) that align with the technical priorities of SAFE-6G. These APIs, once

validated, can be proposed for inclusion in the broader Open CAPIF ecosystem, enhancing interoperability and supporting the evolution of service-based architectures in future 6G networks

SAFE-6G

1/1/2024 - 31/12/2026

SAFE-6G aims to establish a native, user-centric AI/ML cognitive trustworthiness framework. This framework is designed to facilitate the delivery of future 6G critical services sustainably, ensuring safety, security, privacy, reliability, and resilience. To realize this vision, it is crucial to prioritize the openness of network cores and the exposure of capabilities through standardized 3GPP APIs. This approach fosters tighter integration and seamless cooperation between vertical networks. In this context, **OpenCAPIF** will play a pivotal role in SAFE-6G by enabling consistent API exposure that are related to the service mesh networking and the AI-resource orchestration, so that the Cognitive trustworthiness framework could in the end gain awareness of the runtime conditions of the network and therefore to be able to perform the necessary adaptations in order to realise and maintain a pre-defined level of trust.



Figure 4: Screenshot of openCAPIF ecosystem for SAFE-6G

Regarding OpenCAPIF, SAFE-6G project focuses on:

- Exposure of edge-cloud continuum APIs, in order to get information for computing infrastructure.
- API exposure of the user-centric 6G-Core, for instance, NEF functions expose network data and controls for policy adaptation or QoS change.
- API Access for Metaverse information related to the user and the application.

2.3.3.3 NEXT STEPS

The SAFE-6G project has been able to identify potential collaboration opportunities between ETSI and 3GPP, particularly in aligning the work carried out in ETSI (e.g., within OpenCAPIF and other relevant ISGs) with ongoing developments in 3GPP SA3 and SA6. These synergies aim to ensure consistency between application-layer enablers, such as CAPIF, and emerging 6G security architectures, contributing to a more integrated and interoperable standardization landscape.

2.3.4 ETSI – SAI

2.3.4.1 SCOPE

ETSI Technical Committee (TC) SECURING ARTIFICIAL INTELLIGENCE (SAI) aims at developing technical specifications that mitigate threats arising from the deployment of AI, and threats to AI systems, from both other AIs and conventional sources. Whilst in the short to medium term the focus of TC SAI will be on the application of ML, the group shall also give guidance and evaluation reports to ETSI and its stakeholders on the wider developments of AI.

2.3.4.2 ENGAGED WORKS

The following works have been engaged with ETSI SAI:

- Presentation of SAFE-6G works to THALES representative inside ETSI SAI.
- Identification of relevant topics for potential contribution from SAFE-6G project. Currently, SAFE-6G project could contribute to ETSI SAI regarding two axes:
 - Telecom works
 - Explainable AI (XAI) works and results

TELECOM vertical

The general use of AI in all technological activities may cause AI security and privacy issues specific to the telecom industry. In ETSI, SAI specific activity deals with the investigation of security and privacy issues related to the use of AI in the telecom industry sector. Indeed, AI use in telecom industry has shown great potential in assisting with solving problems like (non-exhaustive list):

- Network as a service
- Network optimisation
- Network planning and upgrades
- Automating security operations (anomaly detection, planning mitigation and response)

SAFE-6G activity regarding these security aspects could be relevant for ETSI SAI.

Explainable AI (XAI)

TC SAI has an overall objective around guidance and evaluation of wider development of AI. In this context, ETSI SAI has already highlighted the importance of XAI in the development of AI solutions for a better transparency.

XAI works done in SAFE-6G project focus on the development of an XAI assistant, including LLM part with the following goals:

- Help end-users on choice of the best adequate XAI methods to address their needs
- Offer a better interpretation of the results with textual interpretation.

Regarding the results that will be obtained in SAFE-6G project, and the feedback end-users will give to the XAI assistant, the XAI assistant could be integrated in ETSI SAI as a guidance of the development of AI.

2.3.4.3 NEXT STEPS

SAFE-6G will continue sharing information with ETSI SAI about the results of the project, regarding both identified axes, security of AI in telecom sector and explainability of AI. Project outcomes could be made available to ETSI SAI for potential inclusion/usage in the forthcoming ETSI SAI reports.

2.3.5 CAMARA – QUALITY ON DEMAND (QoD)

2.3.5.1 SCOPE

CAMARA (Carrier-Grade APIs for Applications) is an open-source project under the Linux Foundation that develops standardized, operator-exposed APIs for network-aware application development. By bridging the gap between telecom operators and cloud-native developers, CAMARA ensures that applications can dynamically adapt to network conditions — such as QoS, location, or connectivity status — in real time. The Quality on Demand (QoD) subgroup proposes service APIs for QoD. This subgroup provides the users with the ability to: i) set quality for a flow within an access network connection (e.g. mobile device connection or fixed access between a home gateway and the service providers gateway router); ii) get notification if the network cannot fulfil.

2.3.5.2 ENGAGED WORKS

SAFE-6G project proposes to monitor CAMARA service APIs for QoD sub-project. Works have been engaged to get familiar with CAMARA service APIs for QoD (set quality for a flow within an access network connection, get notifications if the network cannot fulfil etc.). Work is in progress, on the 5G openness of QoD related APIs.

2.3.5.3 NEXT STEPS

For the next steps, the plan is to monitor and align API requirements, enabling seamless access to telco network capabilities (5G and 6G).

Another goal is to extend the Camara Initiative APIs, offering unified developer APIs towards project's components/5G openness. CAMARA APIs can play a vital role in exposing trust-enhancing features to user-centric applications like XR interfaces or trust-aware services deployed across the edge-cloud continuum.

2.3.6 ENISA – EMERGING TECHNOLOGIES

2.3.6.1 SCOPE

The goal of the Union's ENISA agency is to raise the standard of cybersecurity throughout all of Europe. ENISA supports European Union (EU) cyber policy, works with Member States and EU agencies to improve the cybersecurity of ICT products, services, and processes with cybersecurity certification schemes, and aids Europe in preparing for future cyber challenges.

ENISA remains alert and prepared with the best up-to-date information and advice concerning cybersecurity developments in critical emerging areas such as the IoT, 5G communications, ML and AI. Indicative of this targeted focus was ENISA’s Artificial Intelligence Threat Landscape report of late 2020 and Supply Chain Threat Landscape of 2021, as well as the works of ENISA on IoT (baseline security recommendations, secure software development lifecycle and Industry 4.0).

2.3.6.2 ENGAGED WORKS

A webinar was organized between SAFE-6G and ENISA in October 2024. The goal was to present SAFE-6G activity and to identify topics for collaboration.

Some initial ideas have been proposed:

- AI as a tool to support trustworthiness of 6G systems.
- Threat landscape for user-centric and AI-assisted 6G systems.
- Trustworthiness dimensions for 6G systems.

2.3.6.3 NEXT STEPS

SAFE-6G will continue sharing information with ENISA about the results of the project. Where feasible, the work conducted within the project and its outcomes could be made available to ENISA for potential inclusion/usage in the forthcoming ENISA reports.

2.4 CONCLUSION AND NEXT STEPS

2.4.1 ENGAGED WORKS

Up to now, SAFE-6G project standardization works focused on initial exchanges with four SDOs and relevant initiatives. **¡Error! No se encuentra el origen de la referencia.** summarizes the project results that could be pertinent for the SDOs/relevant initiatives activities:

<i>SDO/Relevant initiative</i>	<i>Engaged project works with SDOs/Relevant initiatives</i>
3GPP SA 1, 3 & 6	<ul style="list-style-type: none"> • Activity monitoring regarding: Mission-critical services, proximity services security and AI/ML security, landscape relations with OpenAPIF
ETSI OCP	<ul style="list-style-type: none"> • Contribution to the ongoing development of Common API Framework (APIF) specifications • Development of new APIs
ETSI SAI	<ul style="list-style-type: none"> • Activity monitoring regarding: AI security in Telecom sector, guidelines for trustworthy AI (explainable AI – XAI)
CAMARA	<ul style="list-style-type: none"> • Activity monitoring regarding: CAMARA service APIs for Quality of Demand (QoD) • API alignment for QoD inside the project
ENISA	<ul style="list-style-type: none"> • Activity monitoring regarding: AI for trustworthiness 6G systems

Table 3: Engaged works with SDOs and relevant initiatives

2.4.2 NEXT STEPS

Table 4 summarizes the next steps for already engaged works with SDOs/relevant initiatives:

<i>SDO/Relevant initiative</i>	<i>Next Steps</i>
3GPP SA 1, 3 & 6	<ul style="list-style-type: none"> Align project activity with key standardization topics defined in Release 19 and 20 Monitor and contribute to SA1 and SA3 Contribute to SA3 and SA6 around OpenCAPIF regarding service enablers and API frameworks
ETSI OCP	<ul style="list-style-type: none"> Contribute to OpenCAPIF with SA3 and SA6 regarding service enablers and API frameworks
ETSI SAI	<ul style="list-style-type: none"> Monitor the activity and propose projects results to be integrated in ETSI SAI publications
CAMARA	<ul style="list-style-type: none"> Monitor and align API requirements Offer unified developer APIs towards project's components/5G openness.
ENISA	<ul style="list-style-type: none"> Monitor activity and propose projects results to be integrated in ENISA publication

Table 4: Next steps for already engaged works with SDOs/relevant initiatives

These next steps will be refined to identify concrete targets and milestones to achieve them, to ensure that project results could be presented and possibly integrated in some of the SDOs/relevant initiative outputs.

2.4.3 NEW OPPORTUNITIES

Works will also be conducting to enlarge the study of the standardization landscape relevant for the project. For the moment, we try to investigate the possibility to contribute with 3GPP SA 2. Indeed, SAFE-6G project is closely aligned with 3GPP SA2's ongoing work on 6G system architecture, particularly in areas such as AI-driven orchestration, trust and resilience frameworks, and service-based architecture evolution. Results from SAFE-6G—especially the Explainable AI module and the cognitive security orchestrator—will be evaluated for their potential to contribute to SA2 studies supporting a more transparent and adaptive 6G infrastructure.

We also try to enlarge the participation of the SAFE-6G partners in the JU SNS Pre-Standardization Working Group (WG) to better monitor and interact with the WG. One goal could be to target a presentation of SAFE-6G to inform on the project on envisioned contributions (once confirmed and properly defined).

2.4.4 FOLLOW-UP

Regular meetings (each month) are organized in the context of WP6 to analyse SDOs roadmaps and project works and results that could be relevant for the SDOs and relevant initiatives. A follow-up Excel file is also available to document and share all activities related to the standardization process.

3 EXPLOITATION PLANS AND IPR MANAGEMENT

3.1 INTRODUCTION

This section presents the overarching strategy for exploitation and Intellectual Property (IP) management within the SAFE-6G project. It is structured around two mutually supportive layers:

- **Individual exploitation plans**, that reflect each partner’s goals and innovation assets.
- **A joint exploitation strategy**, that supports shared impact through coordinated activities and synergies across the consortium.

Alongside these exploitation activities, the management of IP—encompassing the identification, use and protection of knowledge—is a foundational element that ensures that the project outcomes remain accessible, valuable and aligned with regulatory and ethical principles. IP management in SAFE-6G respects the terms set forth in the **Consortium Agreement (CA)** and the **Grant Agreement (GA)** and is anchored in transparency, fairness and mutual benefit.

DUAL-LEVEL EXPLOITATION FRAMEWORK

The exploitation model in SAFE-6G is intentionally designed as a two-tiered framework, allowing each partner to pursue their own strategic objectives while also contributing to a collective value creation ecosystem:

Individual Exploitation Plans

Each partner has developed an in-depth exploitation plan that reflects their organizational priorities, domain expertise and potential role in future value chains. These plans outline:

- Innovation pathways, such as commercial product development, licensing, open-source contributions, or follow-up research initiatives.
- The relevance of results to existing business models or Research and Development (R&D) agendas.
- An overview of the intellectual property assets involved, including distinctions between **background knowledge** brought into the project and **foreground results** developed through project activities.

Each partner’s IP-related intentions and rights are clearly expressed in these individual plans, which serve as the primary reference for understanding ownership, usage conditions and future exploitation opportunities. These plans have been developed in alignment with the overarching rules and responsibilities defined by the SAFE-6G CA.

Joint Exploitation Plan

At the consortium level, a shared strategy has been established to amplify the collective impact of project outcomes. This includes:

- Exploring business potential using multiple strategic tools, including Lean Business Canvas, SWOT analysis, Porter’s Five Forces and the Llava Matrix.
- Identifying synergies between partner contributions, as demonstrated through joint use cases (e.g., the Industrial Metaverse and Metaverse for Education).
- Supporting market uptake through interoperable toolkits and demonstrators.
- Coordinated efforts in dissemination, stakeholder engagement and alignment with relevant standards and open innovation ecosystems.

This joint strategy is not intended to override individual interests, but to provide an integrated platform for visibility, collaboration and long-term sustainability of the SAFE-6G innovations.

3.2 IP RIGHTS (IPR) MANAGEMENT APPROACH

The management of IP in SAFE-6G is based on shared principles of openness, fairness and respect for each partner’s contributions and obligations. While no single mechanism governs all IP aspects, the following elements ensure a structured and coherent approach:

- **Recognition of IP Rights and Ownership:** Each partner has formally declared their **background IP** at the beginning of the project. The ownership of **foreground IP**—knowledge or assets created during the project—is determined based on contributions and is described in each partner’s individual exploitation plan.
- **Use and Access Conditions:** Access to necessary IP during the project implementation is based on non-commercial terms and follows the conditions specified in the **CA**. Post-project usage rights are defined individually and bilaterally, ensuring flexibility and respect for each partner’s exploitation strategy.
- **Transparency and Good Practice:** Although SAFE-6G does not rely on a centralised IP protection authority or enforcement system, partners are committed to maintaining transparency and cooperation through shared documentation and open dialogue. All exploitation and IPR-related actions are conducted in accordance with the **GA** and any conflict resolution is guided by procedures outlined in the consortium’s internal governance framework.
- **Open Access and Future Reuse:** In support of long-term impact, partners are encouraged to share selected project results—such as datasets, APIs and tools—under open-access terms where appropriate. This supports further research, standardisation and community development in the 6G domain and aligns with broader EU digital sovereignty and sustainability objectives.

In summary, SAFE-6G’s exploitation and IPR strategy is built on clear partner commitments, mutual respect and alignment with the formal agreements that govern the project. While detailed rights, responsibilities and commercial approaches are defined at the individual level, the joint exploitation plan provides a unifying framework to maximise collective visibility, relevance and impact.

3.3 INDIVIDUAL EXPLOITATION PLANS

3.3.1 INTRODUCTION

Following the dual-layer strategy described above, this section outlines the individual exploitation plans developed by each SAFE-6G partner. These plans reflect each organization’s strategic goals, innovation assets and role within the project value chain.

Each partner details:

1. Their intended use of project results (e.g., commercialization, licensing, internal adoption, or further research).
2. The background IP brought into the project and the foreground IP generated.
3. Ownership, access rights and licensing intentions, fully aligned with the CA and GA.

These plans ensure transparency and IP clarity, define how results integrate with existing activities and support the collective impact through synergies identified in the joint exploitation strategy. They also guide each partner’s pathway for sustaining, scaling, or transferring results beyond the project lifecycle.

3.3.2 TELEFONICA EXPLOITATION PLAN

Telefonica, as a key partner in the SAFE-6G project, is contributing advanced technologies that drive innovation and enhance the resilience of next-generation networks. By integrating its unique technological background with forward-looking developments, Telefonica aligns its contributions with both project goals and long-term market opportunities. This exploitation plan details Telefonica’s approach to leveraging its contributions—OpenCAPIF and the Resilience Function—to support technological innovation, industry standards and commercial adoption.

3.3.2.1 BACKGROUND CONTRIBUTION: OPENCAPIF

Telefonica provides **OpenCAPIF**, a management layer enabling efficient API consumption in a 3GPP-compliant format. OpenCAPIF simplifies network resource access for application developers by avoiding one-to-one integration between operators or NEF providers and developers. This background contribution is designed to facilitate interoperability and efficiency in multi-operator environments.

- **Key Features:**
 - Simplifies API consumption for developers in a 3GPP format.
 - Enables scalable integrations between operators and application developers.
- **Usage Conditions:**
 - OpenCAPIF is developed under the Apache License 2.0, ensuring open-source accessibility.
 - Its use in the project is limited to research purposes and not intended for commercial installations.
- **Implementation Limitations:**
 - None specified. OpenCAPIF source code is freely available under its licensing terms.
- **Exploitation Considerations:**

- While no specific limitations for exploitation are defined, its use in SAFE-6G must align with its open-source licensing model.
- **Strategic Alignment:**
 - Telefonica aims to align the exploitation of OpenCAPIF with the broader SAFE-6G goals, ensuring interoperability and maximizing its potential as an enabler for network innovation.

3.3.2.2 FOREGROUND CONTRIBUTION: RESILIENCE FUNCTION

As part of its involvement in SAFE-6G, Telefonica is developing a **Resilience Function** to enhance network adaptability and reliability under dynamic conditions. This component is essential for maintaining trust and resilience in next-generation networks.

Asset #1

- **Asset Name:** Resilience Function
- **Asset Type:** Platform Component (Trust Function)
- **Description**
 - The Resilience Function evaluates and manages network resilience by implementing parameters such as Desired Level of Resilience (dLoR) and current Level of Resilience (LoR).
 - It leverages Resilience Actions to adapt to dynamic network demands, ensuring service quality through traffic prioritization, resource allocation and traffic rerouting.
 - Ensures alignment with trust metrics like Level of Trustworthiness (LoTw) and integrates with the Cognitive Coordinator for effective resource management.

Availability & Protection

- The Resilience Function will be available to SAFE-6G partners through the project GitLab repository.
- IP protection is under evaluation to determine the most suitable safeguarding approach.

Exploitation Conditions & Status

- Currently, no specific commercial limitations have been defined; decisions on distribution models and IP protection are ongoing.
- Development progress: 20% completed.

Strategic Value

Through its contributions to SAFE-6G, Telefónica aims to:

- Enhance API interoperability and network resilience through OpenCAPIF and the Resilience Function.
- Validate these solutions in collaborative real-world scenarios within the SAFE-6G framework.
- Position itself as a leader in trust and resilience solutions for next-generation networks, aligning with evolving 6G standards.

3.3.2.3 EXPLOITATION STRATEGY AND MARKET OPPORTUNITY

Telefonica's SAFE-6G story centers on leveraging its expertise to drive innovation in next-generation networks. The primary market opportunity lies in developing and deploying the Resilience Function, which enhances network reliability and adaptability through trust-based metrics and cognitive coordination.

A secondary opportunity is OpenCAPIF, an open-source API framework that simplifies developer interactions and enables seamless integration in multi-operator environments. OpenCAPIF's 3GPP-compliant format offers scalability and interoperability, which are crucial for the evolution of 6G networks.

Business Opportunities

Telefonica identifies two major business opportunities within SAFE-6G:

- Enhancing network resilience with the Resilience Function, ensuring improved service reliability under dynamic conditions.
- Facilitating API interoperability with OpenCAPIF, streamlining developer integrations and promoting multi-operator compatibility.

Marketable Products & Services

Potential Commercial Offerings:

- Resilience Function: A platform component for dynamic network management, targeting industries requiring high-trust adaptive networks.
- OpenCAPIF: An API Framework for network developers to facilitate multi-operator API integration.

Fit with Telefónica's Portfolio:

- The Resilience Function aligns with Telefónica's focus on AI-driven, trust-based network innovation.
- OpenCAPIF complements Telefónica's existing API management solutions and open-source initiatives.

Path to Market & Intermediate Steps

1. IP & Licensing Strategy: Finalizing licensing and commercialization models for the Resilience Function.
2. Industry Pilots & Validation: Testing solutions in real-world use cases within SAFE-6G (e.g., enterprise, education).
3. Strategic Partnerships: Engaging with network operators, cloud providers and industry players to drive adoption.
4. Commercialization & Monetization: Exploring SaaS models, licensing opportunities and cross-industry applications.

Near-Term Applications

- OpenCAPIF is ready for immediate implementation in existing 5G and evolving 6G networks.

- The Resilience Function can be deployed in pilot programs to enhance network adaptability and dynamic resource management.

Market Size & Total Addressable Market (TAM)

- Estimating the TAM is complex due to rapid technological evolution in 6G and network resilience solutions.

Competitors & Market Segments

- Telecom Operators: Orange, Deutsche Telekom, etc.
- Cloud Providers (Telecom Integration): AWS, GCP, Azure.
- Network Tech Companies: Nokia, Huawei.
- Security Providers: Fortinet, Palo Alto Networks.

Key Differentiation Strategies

- Innovation: Optimizing OpenCAPIF as the standard framework for multi-operator API management.
- Standardization Leadership: Contributing to 6G standards and aligning with ETSI and 3GPP regulations.
- Strategic Alliances: Partnering with leading industry players to drive adoption and regulatory influence.

Standards & Regulatory Impact

- OpenCAPIF aligns with ETSI & 3GPP standards, ensuring industry-wide compatibility.
- SAFE-6G does not currently propose new standards, but Telefónica aims to drive standardization efforts.

Risks & Market Challenges

Opportunities:

- AI-driven innovation in trust and resilience solutions for 6G networks.
- Exploring new use cases in 6G, focusing on automated trust metrics and intelligent resource allocation.

Threats:

- Fast-evolving market may create challenges in time-to-market for innovative solutions.

3.3.2.4 EXPLOITATION PLAN SUMMARY

Telefonica's **SAFE-6G exploitation plan** is centered on leveraging its **OpenCAPIF** and **Resilience Function** contributions to enhance **next-generation network innovation**.

- **OpenCAPIF** is an open-source API framework that facilitates developer integration and interoperability. Telefónica aims to position it as a standardized solution for multi-operator API management.
- The **Resilience Function** improves network adaptability, reliability and trustworthiness, positioning Telefónica as a leader in trust-based AI-driven network management.

By focusing on partnerships, standardization and commercialization, Telefónica seeks to establish itself as a key innovator in the 6G ecosystem, ensuring long-term adoption and market leadership in next-generation network solutions.

Asset Name	Exploitation by	Exploitation Approach	Competition, Strengths, Weaknesses, Risks	IP Protection	Time-to-Market	Targeted Market	Expected ROI
OpenCAPIF	Telefonica and partners	Open-source implementation for developers and operators	Competition: Proprietary API frameworks. Strengths: Fully 3GPP-compliant, open-source. Weaknesses: Limited initial commercial usage. Risks: Market fragmentation and adoption rates.	None specified (open-source under Apache 2.0)	1-2 years	Global telecom operators, software developers	Increased interoperability, enhanced developer ecosystem and indirect monetization
Resilience Function	Telefonica	Commercial product/licensing for dynamic network management	Competition: Solutions from major vendors like Nokia and Huawei. Strengths: Integration of advanced trust metrics and cognitive coordination. Weaknesses: Early development phase (20%). Risks: IP protection uncertainties and scalability.	Under review	Under review	5G/6G network operators, IoT enterprises	High potential ROI from improved network reliability, adaptability and market differentiation

Table 5: Summary of Exploitable Results (Telefonica)

3.3.3 NCSR D EXPLOITATION PLAN

NCSR D, as the Technical Manager (TM) of the SAFE-6G project, provides advanced 5G/6G testbed infrastructure, cloud computing and network programmability capabilities. By leveraging its Athens 5G/6G Platform and developing AI-driven solutions such as the Cognitive Coordinator, NCSR D aims to enable intent-driven functionalities and trust-centric applications. This exploitation plan outlines NCSR D’s background and foreground contributions, business opportunities within SAFE-6G and potential commercialization pathways.

3.3.3.1 BACKGROUND CONTRIBUTION: ATHENS 5G/6G PLATFORM

NCSR D provides the Athens 5G/6G Platform, a comprehensive experimental facility that enables advanced network experimentation and showcases SAFE-6G innovations.

Platform Features

- **5G/6G Testbed Infrastructure:** Backend infrastructure supporting measurements, processing, virtualization and a fully operational 5G standalone (SA) network. The platform is enabled by different core technologies and can expose standardized native APIs.
- **Edge-Computing-Enabled Radio Infrastructure:** Supports low-latency applications through overlapping coverage using gNBs and small cells.

- NEF Emulator: Provides APIs for session setup, QoS management and traffic influence, compliant with 3GPP standards.
- Cloud Computing Resources: Includes OpenNebula, OpenStack, Kubernetes and Docker-based environments.

Implementation Limitations

- Access to the infrastructure is granted via secure encrypted tunnels (VPN) or physical access upon approval.

Exploitation Limitations

- The Athens 5G/6G Platform and associated technologies are strictly available for project purposes and are governed by the CA.
- Commercial use is excluded unless explicitly authorized by a separate agreement.

Strategic Impact

- Provides a trusted testing environment for AI-driven trust-centric functionalities.
- Enables real-world validation of SAFE-6G's AI-powered networking solutions.
- Supports collaboration with industry and standardization bodies such as 6G-IA and ETSI.

3.3.3.2 FOREGROUND CONTRIBUTIONS: AI-DRIVEN SAFE-6G COMPONENTS

NCSR is developing two AI-powered assets to enable cognitive coordination and trustworthiness assessment in SAFE-6G.

Asset #1

- **Asset Name:** Cognitive Coordinator
- **Asset Type:** SAFE-6G Component

Description

- An intent-handling component that interprets trust intent semantics via the AI Chatbot.
- Calculates the requested LoTw and coordinates SAFE-6G functions to transition the system into a trustworthy state.
- Manages classification and reasoning activities to ensure LoTw compliance.
- Uses AI/ML models for classification and regression tasks to generate a non-calibrated Level of Trustworthiness (nLoT).
- Features data preprocessing, trust profiling and intelligent recommendation systems for recalculating LoTw based on past decisions and knowledge base queries.

Availability

- Accessible through SAFE-6G GitLab repositories and project deliverables.

Protection

- The source code is released at SAFE-6G GitLab under a license that specifies a specific protection policy. Currently, Apache 2.0 is the most preferable option, but it is yet to be decided at the project level.

Exploitation Limitations

- Depends on the final licensing option chosen by the project.

Development Status

- 50% complete.

3.3.3.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

NCSR D as TM of the SAFE-6G project, aims at developing an innovative AI-driven Cognitive Coordinator framework that enables user's trust-centric, intent-based 6G networking, where we spot our key exploitation opportunity. Using the Athens 5G/6G testbed, we validate AI/ML-powered trust mechanisms. Our market route includes technology validation, standardization (6G-IA, ETSI) and industry collaboration for commercialization.

Business Opportunities

As a research institute, NCSR D's commercial exploitation will require:

- Spin-off creation to bring SAFE-6G innovations to the market.
- Commercial agreements with external companies.

Potential Marketable Products & Services

- AI-powered trust orchestration for secure, intent-driven 6G networking.
- Network validation, performance testing and security assessments.

Fit within NCSR D's Research Portfolio

- Strengthens NCSR D's expertise in AI-driven network programmability and security.
- Aligns with 6G research, telecom security and enterprise networking.

Path To Market

1. Align SAFE-6G technologies with ETSI, 6G-IA and industry standards.
2. Pilot deployments to validate AI-powered trust mechanisms in enterprise and IoT environments.
3. Engage with partners for commercialization via spin-offs or licensing agreements.

Near-Term Applications

- Deploying the Cognitive Coordinator for real-time trust verification and threat mitigation.
- Enhancing Zero Trust security frameworks in IoT and cloud computing.

Alignment with SAFE-6G Roadmap

NCSR D's contributions align with its focus on:

- User-centric networking solutions.
- Leading AI-driven trust and security innovations.

Technologies & Work Packages

- Cognitive Coordinator (WP4) – AI-driven trust management for secure 6G networking.
- Athens 5G/6G Testbed (WP3, WP5) – Enabling real-world SAFE-6G component validation.
- 6G Infrastructure Monitoring & Programmability (WP3) – Developing real-time network adaptability APIs.
- WP2 Leaders of architecture design.

3.3.3.4 EXPLOITATION PLAN SUMMARY

NCSR D’s exploitation plan in SAFE-6G focuses on leveraging its Athens 5G/6G Platform and AI-driven innovations to advance trust-centric, intent-based networking.

The Athens 5G/6G Platform provides a real-world testbed for validating SAFE-6G technologies, while the Cognitive Coordinator Components enable AI-powered trust evaluation and decision-making.

NCSR D’s key exploitation avenues include technology validation, standardization (6G-IA, ETSI) and industry collaboration. As a research institute, commercialization would be pursued through spin-off creation or partnerships with external companies.

Next steps involve aligning with industry standards, deploying pilot use cases and engaging in commercialization efforts, ensuring NCSR D’s leadership in AI-driven trust management for 6G networks.

<i>Innovation</i>	<i>To Be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Targeted Market</i>
Cognitive Coordinator	NCSR D	AI-driven 6G networking/trust management	Competition: Global telecom vendors, Strengths: AI-based intent-driven trust, Weaknesses: Early-stage development, Risks: Licensing restrictions	Pending review	6G security & automation

Table 6: Summary of Exploitable Results (NCSR D)

3.3.4 THALES EXPLOITATION PLAN

Thales, a key partner in the SAFE-6G project, contributes its expertise in XAI to develop innovative solutions for enhancing trustworthiness in 5G/6G networks. Leveraging its advanced background technologies and further developing cutting-edge components, Thales aims to provide transparency and reliability to AI systems used within the project. Below is a detailed outline of its contributions, forming the foundation for its exploitation strategy.

Background Technologies

1. Shapkit:
 - Open-source Python module for local explanations of ML models using Shapley values.
 - Provides interpretable insights into model predictions.
2. CFKit:
 - Python module (soon open-source) to generate counterfactual examples for classifiers trained on tabular datasets.
3. TSCFKit:
 - Python module (soon open-source) for generating counterfactual examples for classifiers trained on time-series datasets.

Implementation & Exploitation Limitations

- No specific implementation limitations are defined.

- No restrictions on the exploitation of these tools.

These open-source contributions provide a robust foundation for developing transparent and interpretable AI systems within SAFE-6G.

3.3.4.1 FOREGROUND CONTRIBUTION: XAI ASSISTANT

Asset #1

- **Asset Name:** XAI Assistant – AI-powered Trustworthiness Guidance
- **Asset Type:** Platform Component
- **Description:**
 - Develop an XAI assistant to interact with the end-user to select the best XAI techniques to answer end-user needs
 - Provides and deploys XAI techniques tailored to explaining the five 6G trustworthiness functions.
 - Integrates with the Machine Learning Operations (MLOps) framework of the SAFE-6G that is developed in T3.4.
 - Integrates seamlessly with the chatbot within the Cognitive Coordinator, ensuring transparency and trust in AI-driven decisions.

Availability & Protection

- **Access:** The code will be **available to the consortium**, facilitating integration with other project components.
- **IP Protection:** Patent protection is **under investigation** to secure Thales' intellectual property.
- **Exploitation Limitations:** Dissemination and commercial exploitation will depend on the results of the **patent investigation**.
- **Development Status:** 10% complete.

Strategic Goals

Through its contributions to SAFE-6G, Thales aims to:

- Advance explainable AI solutions that enhance trustworthiness and transparency in 5G/6G networks.
- Validate the XAI Assistant in real-world 6G scenarios, ensuring it aligns with SAFE-6G's trustworthiness objectives.
- Investigate patent opportunities to protect and commercialize its innovations.

3.3.4.2 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

Trustworthiness is critical in 6G networks, where end-users need confidence in AI-driven decisions. Thales' XAI Assistant enhances explainability by helping users understand the trustworthiness of AI models deployed in 6G environments.

By combining XAI techniques and Large Language Models (LLMs), Thales sees a strong market demand for explainable AI in telecom security, cybersecurity and automation domains.

Business Opportunities

- XAI Assistant as an AI trust enabler for 6G networks and cybersecurity applications.
- LLM-powered AI transparency solutions for sectors requiring explainability in decision-making.

Potential Marketable Products & Services

- XAI Assistant as an AI-powered trust evaluation tool for Thales' AI security and automation solutions.
- Integration of SAFE-6G XAI solutions into Thales' broader portfolio, enhancing its trustworthiness AI capabilities.

Path to Market & Intermediate Steps

1. Validate XAI Assistant in SAFE-6G through technological partners and end-users.
2. Assess suitable market domains for early adoption (e.g., cybersecurity, automation).
3. Integrate the solution into Thales' AI-driven offerings, ensuring commercial viability.

Near-Term Applications

- Immediate use of the XAI Assistant in Thales AI-driven businesses, particularly in cybersecurity.

Alignment with SAFE-6G Roadmap

Thales' SAFE-6G contributions align with its strategic focus on AI transparency and trustworthiness.

Technologies & Work Packages

- XAI Assistant (T4.1) – Developing xAI algorithms and LLM-based AI transparency mechanisms.

3.3.4.3 EXPLOITATION PLAN SUMMARY

Thales' SAFE-6G exploitation plan focuses on leveraging its expertise in XAI and LLMs to enhance trustworthiness in 6G networks.

The XAI Assistant provides a transparent, AI-driven decision-making tool that ensures end-users understand and trust AI functionalities in 6G. By integrating the XAI Assistant into SAFE-6G's MLOps framework and chatbot interface, Thales strengthens its AI trustworthiness capabilities.

Key exploitation paths include:

- Validation in SAFE-6G, followed by market selection for deployment.
- Integration into Thales' AI security solutions.
- Potential patent protection and commercialization in AI-driven domains.

Thales' AI strategy focuses on making AI transparent and trustworthy. As part of this approach, Thales is committed to AI that provides safe decisions, especially in 6G and cybersecurity.

<i>Innovation</i>	<i>To Be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
XAI Assistant	Thales	Integration in Thales' AI-driven solutions	C: AI technology suppliers, AI S: Thales' trustworthiness expertise, W: Early-stage development, R: Large competitors entering the market	Pending review	1 year (for advanced AI trustworthiness solutions)	AI-driven security, automation and network trustworthiness	High

Table 7: Summary of Exploitable Results (Thales)

3.3.5 INQBIT EXPLOITATION PLAN

InQbit, a key partner in the SAFE-6G project, contributes to advanced cybersecurity training, simulations and blockchain-enabled Self-Sovereign Identity (SSI) solutions. Through a combination of established background technologies and cutting-edge foreground contributions, InQbit aims to address challenges in secure identity management, network security and trust-based infrastructure. The following exploitation plan outlines InQbit’s contributions and strategic approach for capitalizing on its innovations within SAFE-6G and beyond.

3.3.5.1 BACKGROUND CONTRIBUTIONS

InQbit provides advanced tools and computational resources as its background contribution, enabling cybersecurity simulations and resource provisioning:

1. Cyber Range and Gaming Platforms

- Includes Capture-the-Flag (CTF) platforms for developing and deploying cybersecurity exercises.
- Cyber Gaming platforms for simulating cyberattacks, supported by extensive libraries of cybersecurity scenarios.

2. Cloud and HPC Infrastructure

- Computational resources provisioned through cloud and high-performance computing (HPC) infrastructure, enabling secure, scalable operations.

Implementation and Exploitation Limitations

- Access to computational infrastructure is controlled via secure encrypted tunnels (VPNs).
- Cyber Range and Gaming platforms are made available in binary format on an “as-is” basis for project purposes only.
- Access rights for exploitation purposes are provided under the CA, excluding commercial use unless a separate exploitation agreement is signed.
- Commercial licensing will be available for exploitation during and after the SAFE-6G project.

Through these contributions, InQbit provides a robust foundation for cybersecurity and blockchain-based innovations within the SAFE-6G project.

3.3.5.2 FOREGROUND CONTRIBUTIONS

InQbit is developing three key assets within the SAFE-6G project to advance SSI functionality and blockchain interaction.

Asset #1

- **Asset Name:** Decentralized identifier (DID) Registry (SSI Smart Contract)
- **Asset Type:** Building Block
- **Description:** Enables the creation of a DID registry as part of the SSI infrastructure for user-centric security functions.
- **Availability:** Accessible via GitLab.
- Licensing agreements.
- **Exploitation Limitations:** Asset currently supports CRUD (Create, Read, Update, Delete) operations, with further logic to be developed later in the project.
- **Status:** 80 % complete.

Asset #2

- **Asset Name:** verifiable credentials (VC) Registry (SSI Smart Contract)
- **Asset Type:** Building Block
- **Description:** Supports the creation of a VC registry, essential for SSI infrastructure.
- **Availability:** Accessible via GitLab.
- **Protection:** Licensing agreements.
- **Exploitation Limitations:** Asset currently supports CRUD operations, with plans for more complex SSI functionalities later in the project.
- **Status:** 80 percent complete.

Asset #3

- **Asset Name:** HTTP Gateway (Blockchain)
- **Asset Type:** Application
- **Description:** Provides interaction capabilities with the blockchain network and deployed smart contracts.
- **Availability:** Accessible via GitLab.
- **Protection:** Licensing agreements.
- **Exploitation Limitations:** No specific limitations mentioned at this stage.
- **Status:** 30 % complete.

Strategic Goals

Through its contributions to SAFE-6G, InQbit aims to:

- Advance blockchain-enabled SSI infrastructure for enhanced security and identity management.
- Validate its Cyber Range and Gaming platforms in collaborative scenarios to support real-world cybersecurity training and simulations.
- Establish clear pathways for commercialization, aligning with its licensing and operational models.

3.3.5.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

InQbit's role in the SAFE-6G project is focused on the development of a blockchain-based identity management and security audit platform, designed to seamlessly integrate within the user-centric 6G packet core. By leveraging advanced open-source technologies such as Hyperledger Fabric (for blockchain infrastructure and smart contracts) and Hyperledger Aries (for Self-Sovereign Identity agents compliant with World Wide Web Consortium (W3C) standards for Decentralized Identifiers and Verifiable Credentials), InQbit addresses critical challenges in identity management and cybersecurity. The developed solution emphasizes creating a blockchain-based SSI infrastructure featuring smart contracts for security audits and tokenization of actions within a zero-trust architecture. The standout exploitation opportunity lies in utilizing these technologies to enhance identity management by granting users full control over their identities and associated actions. Additionally, the development of this platform significantly strengthens and evolves our cybersecurity capabilities, positioning itself as a transformative solution for secure and reliable 6G networks.

Business Opportunities

SAFE-6G presents multiple business opportunities for InQbit:

- Development of secure, user-centric, identity management services.
- Blockchain-based tools for regulatory compliance and audit security.

- Providing secure and reliable blockchain-based infrastructures for 6G networks and nodes.
- Commercialization of the SSI infrastructure for industries requiring secure identity management.

Marketable Products and Services

- Blockchain-Based SSI Solutions including agents, smart contracts and a blockchain-based verifiable data registry.
- Security Audit Smart Contracts that provide a network monitoring system for security audits and ensure transparency and compliance.
- AI Trust Agents that enable intelligent decision-making and resource management in trust-based security systems.

These products align with InQbit's cybersecurity and blockchain expertise, focus on the market's increasing demands in 6G network security, and expand InQbit's portfolio to include cutting-edge 6G technologies.

Path to Market

A step-by-step approach will be followed for market entry:

- Complete SSI scenarios and blockchain testbeds for the project.
- Develop and demonstrate interoperability with 6G network standards and deploy in pilot projects.
- Identify possible business opportunities and market impact.
- Commercialize the components through partnerships and licensing agreements.
- Engage with industry partners for real-world validations.

Near-Term Applications

SAFE-6G technologies with immediate application include:

- Secure blockchain communications for critical infrastructures.
- Privacy-preserving identity management for consumers and enterprises.
- Enhanced cybersecurity for emerging IoT ecosystems in 6G networks.

Market Size and Total Addressable Market

The market for self-sovereign identity (SSI) is expected to grow significantly over the next several years. The SSI market size is projected to expand from USD 1.8 billion in 2024 to [1] USD 47.1 billion by 2029, exhibiting a remarkable Compound Annual Growth Rate (CAGR) of 90.5% during this period. Similarly, [2] projects an increase from USD 4.0 billion in 2024 to USD 717.1 billion by 2032, with a CAGR of 91.20% by 2032. This significant growth is being driven by:

- Rising concerns about data privacy and security.
- Shift to decentralized identity models.
- Growing demand for seamless identity verification solutions across multiple industries.

Regional Insights

- North America: Currently the largest market share holder due to advanced technological infrastructure, high adoption rates among enterprises and robust privacy regulations like CCPA. The region is driven by strong investments in cybersecurity and identity management technologies.
- Europe: A key market for SSI adoption, supported by stringent data protection laws like GDPR and ongoing digital identity initiatives across EU member states. Europe's focus on

decentralized identity naturally aligns with InQbit's blockchain-based SSI solutions and services.

- Asia-Pacific: Expected to exhibit the fastest growth rate, fueled by increasing digital transformation in countries like China, India and Japan. High smartphone penetration and a surge in government-led digital identity programs create significant opportunities.
- Rest of the World: Emerging markets in Latin America and Africa are witnessing growth in digital identity adoption, driven by advancements in mobile technology and digital banking systems.

Current Market Position

InQbit is establishing itself as an industry innovator in R&D, particularly within the European Union's Horizon Europe framework. InQbit, known for its innovative approaches and competitive participation in high-profile projects, is emerging as a key player in next-generation technology domains. The company has successfully secured funding for a number of EU-funded initiatives, demonstrating its commitment to advancing cutting-edge technologies and encouraging innovation. InQbit's portfolio includes groundbreaking contributions in 6G research, blockchain technology, cybersecurity and artificial intelligence. Its participation in flagship projects such as SAFE-6G demonstrates its ability to tackle complex issues in secure network architectures and identity management. Through strategic partnerships and collaborations with key industry players, InQbit has established itself as a trusted innovator driving technological excellence and market leadership.

Impact on Business Performance

The project's innovations are expected to have a positive impact on the gross margin and net profit by expanding our product offerings and entering new markets, resulting in a 5-10% revenue increase within two years of completion.

Organization's Roadmap

InQbit's roadmap focuses on the phases of development, validation and commercialization of the blockchain-based identity and security audit solutions designed and developed within SAFE-6G:

1. 2024-2025: Development & Initial Testbeds - Complete the SSI infrastructure and blockchain-based security audit platform. Demonstrate interoperability with 6G components in pilot environments.
2. 2026: Validation & Optimization - Enhance the AI agent for adaptive security decisions. Conduct scalability and reliability testing with industry partners.
3. 2027: Market Readiness - Secure certifications and compliance with 6G standards. Launch pre-commercial pilots with interested partners.

Alignment with Roadmap:

InQbit's targeted fields and tasks within the SAFE-6G project are closely aligned with its organizational roadmap and long-term strategic goals:

- Blockchain-Based Identity Solutions: The development of the SSI infrastructure and security audit mechanisms for the user-centric security functions, fully aligns with InQbit's focus on decentralized, user-centric cybersecurity technologies.
- Integration with Emerging 6G Standards: The project's emphasis on 6G interoperability through OpenID Connect and CAPIF/NEF integration are in line with InQbit's goal to integrate

decentralized identity and develop next-generation network-ready security solutions for 6G systems.

- AI-Driven Security Enhancements: The creation of a local AI agent for dynamic resource and trust management reflects InQbit's commitment to advancing intelligent, adaptive security solutions.

Technologies and Work Packages

InQbit is the leader of WP4 in the SAFE-6G project, focusing on the development of the cognitive coordinator, user-centric trust function and XAI. The main tasks of InQbit include T1.4: Ethics, Legal Aspects and Data Management Plan, addressing the regulatory and ethical foundations of 6G systems and T4.3: User-Centric Security Function, which involves the creation of a user-centric blockchain-based identity and security solution, utilizing SSI frameworks and AI-driven trust agents.

Current State of the Art

Identity management and cybersecurity systems for next-generation networks are driven by advancements in decentralized identity solutions, blockchain technology, zero-trust architectures and AI-driven security systems. SSI frameworks, such as Hyperledger Aries and Indy, align with W3C standards for DIDs and Verifiable Credentials (VCs), empowering users with greater control over their identities. Blockchain platforms like Hyperledger Fabric provide tamper-proof, transparent systems for recording security audits and identity transactions. Zero-trust frameworks emphasize continuous verification of users and devices, while AI models like Random Forest classifiers and time-series forecasters enable intelligent resource allocation and real-time threat detection. Despite these advancements, many existing solutions lack seamless integration with emerging 6G network technologies, which are critical for achieving interoperability and scalability. Decentralized and zero-trust systems often face high implementation complexity and resource demands, limiting widespread adoption. InQbit's contributions to the SAFE-6G project aim to address these gaps by enabling blockchain-based SSI infrastructures and AI-driven adaptive security mechanisms, advancing the capabilities of 6G networks and setting new benchmarks for network security.

Competitor Analysis

The identity management and cybersecurity for next-generation networks is highly competitive with key players like IBM, Microsoft offering advanced blockchain solutions integrating SSI and zero-trust principles, while Cisco, Nokia and Ericsson lead the markets of network security and telecommunication infrastructures. These competitors focus on scalability, interoperability and robust security frameworks. InQbit differentiates itself with its blockchain-based SSI infrastructure by emphasizing on the user-centric aspect, with enhanced smart contract privacy and seamless 6G integration. Leveraging SAFE-6G's focus on innovative technologies and interoperability, InQbit is well-positioned to address market gaps, form strategic telecom partnerships and strengthen its competitive advantage in delivering next-generation security solutions.

Standards and Regulatory Impact

- Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs): Governed by W3C [3], these standards provide a foundation for secure, user-centric identity management.

- **Zero-Trust Security Models:** Defined by NIST [4] and industry-specific frameworks, ensuring continuous verification across systems.
- **6G Network Standards:** Proposed by 3GPP and ETSI, focusing on interoperability, security and scalability in next-generation networks.

Controlling Bodies:

- **W3C:** Oversees DIDs and VCs for decentralized identity.
- **3GPP:** Develops standards for 5G and emerging 6G networks.
- **ETSI:** Focuses on telecommunication interoperability and security.

Application Environment Changes

Several of the evolving trends in the application environment that could significantly impact the SAFE-6G objectives are the following:

- **5G to 6G Transition:** SAFE-6G's goals are centred on improving interoperability, scalability and user-centric security solutions, all of which are demanded by the continuous transition from 5G to 6G networks. Adoption of the relevant developed solutions heavily depends on this.
- **Increased IoT Adoption:** Secure communication protocols and robust, decentralized identity management platforms are essential for the growth of IoT devices. SAFE-6G's security-function will give major emphasis on the blockchain network and SSI technologies utilized, to align with these needs.
- **Growth of Edge Computing:** The shift towards edge computing emphasizes low-latency, secure and localized processing, making SAFE-6G's blockchain-based audits a critical component, while zero-trust architectures will play a major role in the evolution of next-gen user-centric network models.
- **Evolving Regulatory Landscape:** Compliance-driven solutions are required due to stricter privacy and security laws like the GDPR and new 6G-specific regulations. This requirement is reinforced by SAFE-6G's conformance to international standards.
- **Rising Cybersecurity Threats & Evolving Threat Landscape:** Increasing sophistication of cyberattacks highlights the need for adaptive, AI-driven security measures, reinforcing SAFE-6G's commitment to zero-trust principles and intelligent resource management.

Opportunities and Threats

Opportunities

The adoption of 6G technologies and increasing demand for data privacy present significant opportunities for InQbit. The market for InQbit's blockchain-based innovations is favorable due to the growing interest in decentralized security solutions and SSI frameworks. Partnerships with telecom operators, government agencies and technology providers offer pathways to scale and deploy solutions widely. Additionally, active participation in standardization efforts through bodies like W3C and 3GPP positions InQbit as a leader in influencing the development of safe, user-focused networks.

Threats

There are still risks in the current competitive environment with well-established firms like Microsoft and IBM, already using their resources to gain market share. Operational difficulties may arise from adhering to changing international regulations and staying relevant may require constant innovation due to the quick development of blockchain and cybersecurity technologies. Furthermore, early

adoption and deployment of 6G technologies may be struck by delays specifically when it comes to standardization. Proactively addressing these issues will be essential to InQbit's success.

3.3.5.4 EXPLOITATION PLAN SUMMARY

InQbit’s exploitation plan focuses on leveraging its contributions to the SAFE-6G project to develop and commercialize innovative solutions in blockchain-based identity management and security audit systems. These include a SSI framework aligned with W3C standards, smart contracts for transparent and immutable security audits and AI-driven trust management systems integrated within a zero-trust architecture. By combining these advancements, InQbit aims to address critical challenges in 6G network security and identity management. The standout exploitation opportunity lies in deploying the SSI framework within user-centric 6G cores through the user-centric security function, empowering individuals with full control over their identities while ensuring regulatory compliance and enhanced security. InQbit will target key industries such as *telecommunications, healthcare and critical infrastructure*, where secure and decentralized identity management solutions will have centrepiece role. The commercialization strategy will involve pilot deployments with industry partners, achieving compliance with international standards and licensing proprietary technologies. The roadmap includes phased development, testing and market entry, with an emphasis on scalability, interoperability and the user-centric paradigm. Aligning with global trends, including the 5G-to-6G transition, rising cybersecurity threats and growing demand for decentralized identity solutions, InQbit is well-positioned to lead new advancements in the SSI and cybersecurity markets. The projected market impact includes significant revenue growth (10%), strengthening industry partnerships and having a key role in shaping the future of secure 6G user-centric networks.

Innovation To Be Exploited By	Type of Exploitation	Competition, Strengths, Weaknesses, Risks (C, S, W, R)	Conflicting IP	Time-to-Market	Targeted Market	Expected ROI	
Blockchain-Based SSI Framework	InQbit	Product, Licensing, SaaS	C: IBM, Microsoft S: Compliance with W3C standards, W: Market penetration R: Rapid tech evolution	None	2-3 years	Telecom, Healthcare, Critical Infrastructure	10-15% growth
Smart Contracts for SSI & Security Audits	InQbit	Product, Licensing, Consulting	C: Audit tool vendors S: Transparency via blockchain W: Scalability R: Standardization delays	None	2 years	Enterprises, Compliance & Audit Sectors	Recurring revenue from licenses
AI-Driven Trust Agents	InQbit	Product, Licensing, Integrated Services	C: AI security platforms S: Custom AI integration W: Initial complexity R: Model standardization	None	3 years	Telecom operators, IoT	10-15% growth

Table 8: Summary of Exploitable Results (INQBIT)

3.3.6 EVIDEN EXPLOITATION PLAN

Eviden, a leading partner in the SAFE-6G project, provides advanced AI/ML and identity management technologies to address key challenges in network orchestration and security. By leveraging its existing technologies and developing innovative solutions, Eviden aims to contribute to the advancement of

next-generation networks while aligning its outputs with internal business strategies and market opportunities. Below is a detailed description of Eviden’s contributions, forming the foundation of its exploitation strategy.

3.3.6.1 BACKGROUND CONTRIBUTIONS

Eviden provides two critical technologies as part of its background contribution:

1. MLOps Framework

- Description: Supports the lifecycle management of AI/ML models across multiple domains, from design and training to deployment in production. It is infrastructure-agnostic, enabling in-network training and seamless integration into various environments.
- Limitations for Implementation & Exploitation:
 - The framework relies on open-source libraries and may face limitations due to the unavailability of sufficient data for training and evaluation, potentially affecting accuracy and robustness.
 - Access rights for exploitation are to be agreed upon on an ad hoc basis.
 - No provision of source code.

2. Self-Sovereign Identity (SSI) Solution

- Description: Comprises components for managing decentralized identities, including registries (DID, schemas, revocation), VCs and authentication/authorization functionalities.
- Limitations for Implementation & Exploitation:
 - Architecture and use case descriptions are currently unavailable.
 - The SSI solution is accessible to project beneficiaries on a royalty-free basis, limited to the duration and scope of the project.
 - Access rights for further exploitation outside the project will be discussed separately.

Through these contributions, Eviden provides foundational tools to enhance AI/ML capabilities and secure identity management within the SAFE-6G ecosystem.

3.3.6.2 FOREGROUND CONTRIBUTIONS

Eviden is developing two key assets within the SAFE-6G project to address advanced challenges in AI/ML orchestration and decentralized identity management:

Asset #1

- **Asset Name**: Evolved MLOps Framework
- **Asset Type**: Platform Component
- **Description**: The MLOps Framework manages the full lifecycle of distributed AI/ML models, including their creation, orchestration and deployment. It will be adapted to the needs imposed by the SAFE-6G project (i.e., serving training models in containers).
- **Availability**: The MLOps Framework will be accessible for SAFE-6G project members and integrated into project tasks.
- **Exploitation Limitations**:
 - Access rights for exploitation are to be agreed upon on an ad hoc basis.

- No provision of source code.
- Alignment with Eviden’s internal business units and product lines.
- **Status:** In evolution.

Asset #2

- **Asset Name:** Evolved SSI Solution (to be reviewed by Keynectis)
 - Asset Type: Platform Component / Building Block
- **Description:**
 - Includes core components for decentralized identity management, such as registries (DID, schemas, revocation), DID, VCs and authentication/authorization functionalities.
 - Will integrate into InQbit’s blockchain solution and LoTw framework defined in SAFE-6G, mainly focusing on the security user-centric function.
- **Availability:** The solution will be accessible via SaaS deployment.
- **Protection:** Intellectual property is protected under the GA, with potential for further restrictions or patenting in the future.
- **Exploitation Limitations:**
 - Access is limited to the project duration and scope. Further exploitation rights will be discussed as needed.
- **Status:** 25 % complete.

Strategic Goals

By integrating its background technologies and developing new foreground assets, Eviden aims to:

- Advance AI/ML orchestration capabilities to support network resilience and efficiency.
- Establish secure, decentralized identity management solutions to enhance trust in next-generation networks.
- Align its contributions with internal product lines and business strategies for seamless market integration.

3.3.6.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

The SAFE-6G project provides Eviden with opportunities to:

- Encourage knowledge and technology transfer inside and outside the organization.
- Promote innovation inside the organization, potentially enhancing the company’s portfolio of products and services.
- Explore new funding opportunities, fostering collaboration and innovation across Europe.

Specific opportunities within SAFE-6G include:

As stated above, SAFE-6G project is a great opportunity for Eviden to be up to date with the latest trends and technologies related to several topics of interest for the company (i.e., MLOps and SSI solutions). This may result in improving somehow the organization’s portfolio of products and services. However, this must be further evaluated.

- MLOps Framework:
 - Enhancing current Eviden’s portfolio of MLOps solutions.
 - Consulting services opportunities.
- SSI Solution:

- Extend Eviden’s portfolio digital identity management solution.
- Ensure compliance with European regulations and standards on digital identity wallet and 6G network.

Marketable Products and Services

During the project, Eviden will try to evolve two existing assets, the MLOps Framework and the SSI System, both developed in the context of the Eviden Big Data & Security (BDS) department. BDS mission is to combine advance computing and security to provide trusted data intelligent, with AI/ML at the heart.

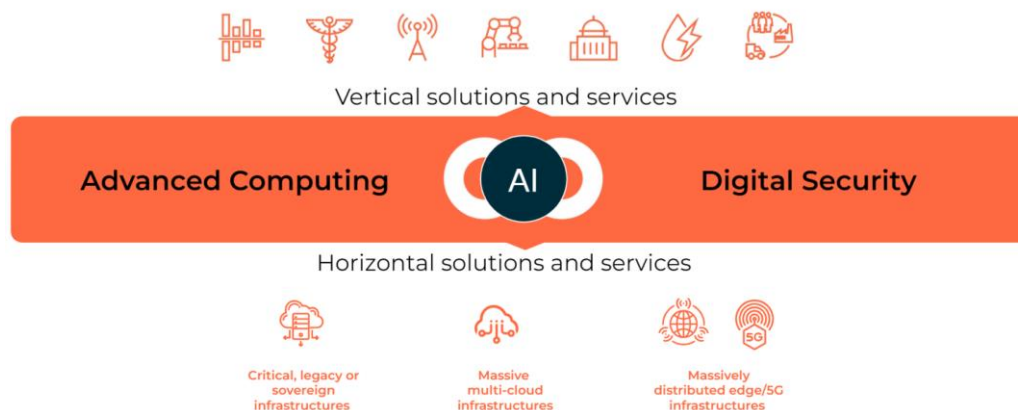


Figure 5: Eviden Big Data & Security department

BDS value proposition is a unique synergistic alliance of computing and security solutions:

- **Advance Computing:** Bringing intelligence and AI accross the digital continuum.
 - High-Performance Computing: high-performance solutions and services to help large enterprises and governments master the race to simulation, AI and Quantum.
 - Edge/AI: Ready to use data intelligence, vertical AI applications and computer vision and Eco-Design Cloud Solutions.
 - Business computing: Critical and in-memory computing on-premises or in the cloud.
- **Digital Security:** Delivering end-to-end zero trust, business continuity and resilience.
 - Mission Critical Systems: Mission-critical vertical solutions combining Comm, Systems, IT and platforms for strategic apps in Defense and Aerospace, Public Safety, Energy and Transport.
 - Cyber-security services: End-to-end services across all continents from Consulting and Integration to Managed Services leveraging our unique Alsaac technologies for AI-powered Managed Detection and Response.
 - Cyber-security Products: Sovereign Cyber technologies in identities & data protection with Digital ID & IAM and cryptography.

Both assets, the **MLOps Framework** and the **SSI Solution**, perfectly fits within the BDS vision.

Eviden is a well-recognized leader in the Digital Identity Product & and Services in Europe and has a range of digital identities solutions (PKI, CMS, etc.). The aim of SAFE-6G participation is to enhance our

portfolio with decentralized identities management. Eviden invests in Research & Development for SSI to be aligned with the newly published eIDAS v2 regulation and the latest protocols and standards listed in the European ARF (Architecture Reference Framework).

Path to Market

The commercialization of SAFE-6G innovations involves:

- **MLOps Framework:** First step would be to analyse if the MLOps Framework could be integrated within existing BDS solutions and how. Then, the MLOps Framework should be taken to a production readiness level and its market readiness evaluated in order to determine if the asset (or any of its features) is ready to face competition, satisfy demand, generate revenue, etc.
- **SSI Solution:** The first step is to industrialize our solution and validate our interoperability through the SAFE-6G use cases and develop our partnership in this field.

Total Addressable Market (TAM)

MLOps Framework: According to Machine Learning Operations Market Size | CAGR of 43.2% [5] :

- The Global MLOps Market size is expected to increase from USD 2.08 Billion in 2023 to around USD 75.42 Billion by 2033, growing at a CAGR of 43.2%.
- As of 2023:
 - By market component, the Platform segment was the winner (versus the Service segment) with a market share of more of 70%.
 - By deployment mode, the Cloud segment led the market with over 68% of the market share (versus the On-premise segment).
 - By organisation size, Large Enterprises held a dominant market position in 2023, capturing more than 71% of the market share.
 - By vertical, the Banking, Financial Services and Insurance (BFSI) sector led the adoption of MLOps, capturing over 20% of the market share.
 - By region, North America held a dominant market position with more than 41% share, reaching USD 0.8 billion.
- **SSI Solution:** The contributions on SAFE-6G project will make it possible to address different areas: telecoms, banking, education, initially mainly in Europe.

Technologies and Work Packages:

Eviden is contributing to the design of the SAFE-6G Architecture (WP2) as well as to the design and development of the project MLOps framework (WP3) and to the Authentication & Key Agreement Protocols by adopting SSI (WP4). We also have effort in WP5, related to Integration, validation and pilots.

In WP3, an existing MLOps framework for the training and serving of ML models is being adapted to the needs of the project. Its evolution is still under discussion.

Regarding our participation in WP4, our proposal aims to enable secure and user-centric communication between user equipment and the 6G infrastructure in a manner that preserves user privacy. The technologies we aim to integrate include the creation of authorizations in the form of Verifiable Credentials (W3C-compliant) and decentralized identities (also W3C-compliant, with a decentralized resolution method currently under evaluation to align with the registry and blockchain solution provided by INQBT). This is complemented using standard protocols such as OID4VC, OID4VP,

OID4VCI and SIOPv2 with OpenID Connect to enable several authentication and authorization mechanisms with respect to the Safe-6G project and use cases.

Current Market Position

Eviden is a clear leader in the Advance Computing and Digital Security market:

- **Advance Computing:**
 - High-Performance Computing: #3 Worldwide #1 EU (Source: Hyperion).
 - Edge/AI: Leader of Leaders (Source: ISG).
 - Business computing: #2 Worldwide in High End (Source: Gartner).
- **Digital Security:**
 - Mission Critical Systems: Top Player.
 - Cyber-security services: #1 in Europe in Managed Security Services (Source: Gartner).
 - Cyber-security Products: Top player and Leader in Europe (Source: IDC).

In addition, Eviden is currently positioning itself as a partner in a European Large-Scale Partnership (LSP) project within the Digital Ecosystem. We are awaiting a response from the European Commission by mid-2025, positioning ourselves as both a specifier and implementer of digital identity solutions for credentials issuance and credentials verification, acting as a real technology provider of innovative solutions. Our target market is therefore the European market, focusing on multiple use cases related to citizen services and travel facilitation.

Current State of the Art:

MLOps Framework

There is currently a huge trend of incorporating AI and ML components into software systems to take advantage of their inferential and predictive capabilities. MLOps has become a popular topic as it proposes practices, processes, techniques and technologies for facing the existing challenges related to the “productionalization” of the AI/ML components, enabling rapid and reliable productionalization of ML systems. MLOps was first proposed by the research community in 2015 as a solution to speed up the ML lifecycle management and to achieve the scalability expected by business applications. Research shows that proper operationalization of ML-enabled systems depends on utilizing such robust MLOps practices, processes and technologies.

However, MLOps spans across a broad spectrum of activities (starting from data collection to model maintenance), a plethora of practices, tools and technologies supporting and automating each of these activities and interdisciplinary collaborations. This complexity and the lack of maturity of the technology are the main reasons why effective adoption is not a reality yet. Organizations follow a different approach for developing and operationalizing ML systems based on their unique use cases and organizational structure [6]

A Multivocal Review of MLOps Practices, Challenges and Open Issues [6] compiles a set of work practices, techniques and technologies that organizations need to implement to enable MLOps:

- Adapting the team structure to the multifaceted challenge that the productionalization of ML models implies.

- Following Work Practices to foster effective collaboration among such diverse stakeholders and enable successful implementation.
- Improving the transparency and provenance across the ML life cycle to help project teams avoid or reduce duplicated work and identify the root causes of potential production issues.
- Continuous monitoring across ML life cycle.
- Systemizing the provisioning and configuration of the infrastructure and environment, as performance of ML models depends not only on the input data and model parameters but also on the software environment surrounding them.
- Systemizing the model deployment (i.e., using software container to package and deploy ML code, abstracting data acquisition, applying patterns for upgrading models.
- Setting up automated pipelines for cross-silo Activities, such as developing and utilizing automated pipelines, optimising and automating MLOps pipeline creation and management, simplifying the integration of software tools and components into MLOps pipelines.
- Abstracting MLOps complexity by using integrated development platforms that provide a collaborative environment for whole-life-cycle-management for ML models and abstract the complexity from end users. On the other hand, functional decomposition and reference architecture of MLOps systems guide the composition or development of MLOps pipelines and platforms depending on domain-specific requirements.

A Multivocal Review of MLOps Practices, Challenges and Open Issues [6] also identifies several additional challenges that hinder teams from efficiently adopting MLOps into their organization's ML-based software system productionalization process. The following table summarizes such challenges and highlights reported solutions from the literature:

	MLOps Adoption Challenges	Primary Aspects	Proposed Solutions
Socio-technical Challenges	Cultural Changes: Disruptions caused by MLOps related culture and work practices in traditional software management process.	Openness and willingness of teams to change [PS103] Continuous collaboration among team members from multiple disciplines [PS104], [PS108] Successful implementation of cultural changes [PS103]	Available MLOps processes, practices and tools to promote collaboration [PS104], [PS108] [PS103], and identify/resolve collaboration conflicts [PS104] Follow a human-centric approach to implement cultural changes [PS154]
	MLOps Fragmentation: Fragmentation of practices, technologies and tools due to rapid growth in MLOps.	Inherent complexity of MLOps [PS154], [PS132] Accidental complexity due to fast evolution of MLOps [PS154]	MLOps Standardization [PS154] Creating domain-specific MLOps reference architectures [PS134], [PS133], [PS127]
	Responsible MLOps: Challenges related to achieving regulatory compliance, AI fairness, transparency, accountability and security throughout the MLOps life cycle.	Lack of expertise and standardized MLOps practices related to compliance, fairness, explainability and security [PS105], [PS121] Limitations in end-to-end MLOps tools for facilitating responsible AI [PS152] [PS114]	Frameworks integrating responsible AI practices into MLOps [PS108], [PS117] Tools for enabling and automating responsible AI practices across ML lifecycle [PS152], and their detailed documentation [PS105]
MLOps Pipeline Related Challenges	Complexity: Complexity of ML pipelines hinders their use during initial stages of the ML development	High setup and maintenance overhead. [PS129] High level of expertise required to operate pipelines. [PS129] High infrastructure costs [PS129]	Frameworks for creating lightweight ML pipelines. [PS129]
	Optimized deployment: Optimal placement of pipeline modules within distributed environments.	Operation across distributed and heterogeneous resources [PS127], [PS128] Manual provisioning of pipelines in distributed and dynamic environments is error prone and sub-optimal [PS127, PS128] Training challenges due to ML models growth [PS126]	Strategic modularization [PS127] Dynamic provisioning of containerized pipeline modules [PS127] Dynamic resource provisioning for parallel or distributed model training [PS126]
	Managing large scale pipelines: Maintaining thousands of production pipelines without failures.	Failure-prone, recurring and inter-dependent production pipelines. [PS131] [PS176] Manual, time-consuming monitoring and resolution of failures. [PS131] [PS177]	Automation of pipeline operation monitoring and failure root cause analysis. [PS131] [PS177]
	Continual learning: Operation of efficient continual learning (online learning) pipelines for high velocity and high volume streaming data	Synchronization between learning, serving and maintenance activities [PS124], [PS125] Overwhelming model updating due to incoming high-velocity data streams [PS125]	Horizontal and vertical scaling of online-learning tasks based on predictions demand, data velocity, and volume [PS125]
	Automation Decision Dilemma: Deciding which activities of the pipelines to automate and which needs human involvement	Automation of certain ML life cycle activities (model development, model validation) reduces incorporation of human judgment which can negatively effect the use of responsible AI [PS110], [PS114]	Design and implementation of pipelines in which the tedious tasks are automated and human insights are incorporated wherever it is needed throughout the lifecycle [PS110], [PS114] [PS117]
	Platform Customization: Decision on whether to use a managed MLOps platform or create a customized platform.	Complexity and cost of managing own platforms add a heavy burden [PS108] Cloud-based managed platforms lacks fine-grain control and customization support [PS108]	Building managed platforms with integration and customization support [PS108] Adopt a modular architecture [PS108] Increase support for open-source ML tools and their integration [PS108]
MLOps Platform Related Challenges	Scalability: Ability of the MLOps platforms to maintain smooth execution of MLOps services as the number of service requests increases.	Lack of scalability as the number of service requests fluctuates in monolithic architecture [PS120]	Using Microservice Architecture for platform design [PS120]
	Artifact Management: Management of data, models and associated meta-information to ensure ML experiment tracking/governance and reproducibility	Challenging versioning, traceability and reproducibility due to increased number of artifacts [PS85], [PS164] Reproducibility based on conjugated management of the related artifacts. [PS122]	Tools/ platforms supporting version controlled and conjugated management of artifacts [PS122]
	Distributed computing environments: Challenges with design, deployment and maintenance of MLOps pipelines in decentralized edge environments	Edge-AI has given rise to paradigms like TinyML, Federated ML at edge, which have MLOps related requirements different from the cloud-based platforms. [PS123]	Build platforms that support MLOps support for usecases such as TinyML and Federated ML at the edge. [PS123]
	Migration to MLOps platforms: Challenges faced by practitioners when integrating existing projects to MLOps platforms	Tedious process of retrieving information from existing project that are required as input for the platform [PS178] Selecting a suitable MLOps platform for the project [PS178] Incompatibility between MLOps and DevOps tools [PS160] [PS19]	Document the ML components and artifacts and use it for migration process [PS178] Selecting a platform based on the architecture of the existing project [PS178] Use tools that offer hybrid CI/CD environment [PS178]

Table 9: MLOps challenges and reported solutions (from literature)

SSI Solution:

As Technology Provider, in addition to Credential Issuance and Credential Verification stack defined in EUDI Wallet ecosystem and ARF, we work to provide Bridging Service to facilitate seamless communication between existing legacy IT systems and EUDI Wallet ecosystem.

Competitors

- MLOps Framework [4]

The key players in the MLOps market are often well-known technology companies with a proven track record in delivering solutions and services related to ML/AI. Their reputation and brand recognition contribute to their credibility in the market. They provide comprehensive MLOps offerings that cover various aspects of the ML lifecycle, such as model development and training, deployment and management, model monitoring and optimization and collaboration and automation tools.

Among top key players we can mention:

- Akira AI
 - Cloudera Inc.
 - Alteryx Inc.
 - IBM Corporation
 - Amazon Web Services Inc.
 - Databricks Inc.
 - DataRobot Inc.
 - GAVS Technologies
 - Microsoft Corporation
 - Google LLC
 - Neptune Labs
 - H2O.ai
 - Other Key Players
- SSI Solution:
The decentralized identity landscape is evolving rapidly, with several key players leading innovation in this space. These organizations focus on developing privacy-preserving identity management solutions and advanced credentialing mechanisms using W3C Verifiable Credentials and Decentralized Identifiers (DIDs). Numerous Blockchain-enabled SSI ecosystems are also contributing significantly to this evolution and are de facto competitors.

In addition to these market players, companies actively participating in the standardization workshops of W3C, IETF, OpenID Foundation and the Decentralized Identity Foundation are also significant competitors. Their involvement in defining the standards gives them a strategic advantage, as they often become the first implementers of solutions compliant with these emerging standards.

Competitors in the SSI and decentralized identity market stand out by offering:

- Full compliance with emerging standards, including W3C Verifiable Credentials and DIDs.
- Blockchain-based registries for decentralized trust management, ensuring secure and transparent identity verification processes.
- Support for multiple authentication protocols, including OpenID Connect (OIDC), OAuth 2.0 and SIOPv2, enabling interoperability across various platforms.
- Privacy-preserving mechanisms, ensuring user data protection while adhering to strict data protection regulations such as GDPR.

Standards and Regulatory Impact

- MLOps Framework:

The MLOps framework will consist of a gathering of several open-source projects that solve by themselves different stages of ML lifecycle. The cornerstone of the framework will be Kubeflow, an open-source platform based on Docker containers and Kubernetes for building ML workflows. Another series of modules are being developed around this platform to provide the framework with the desired functionality, such as Minio, Tensorflow Serving or Torch Serve [[7]].

The benefits offered by open-source software are well-known [8] : cost, security in the sense that bugs and defects can be identified and fixed quicker, quality due to the number of developers adding new features or enhancing existing ones, customizability, reliability as it takes less time to identify and resolve these bugs and defects, as user and technical support from the open-source community.

- SSI Solution:
 - Verifiable Credential Issuance: we implemented OpenID for Verifiable Credential Issuance protocol.
 - Verifiable Credential Verification: we implemented OpenID for Verifiable Presentation & Self-Issued OpenID Provider protocols. We also implemented the Presentation Exchange v2.0 specification, enabling Verifier to flexibly express their verifiable presentation requests.
 - Verifiable Credential Lifecycle Management: we implemented the Verifiable Credential Status List 2021 and Bitstring Status List specifications.
 - Verifiable Credential Formats: we implemented IETF SD-JWT VC, W3C Verifiable Credential Data Model v2.0 and ISO/IEC 18013-5 mDL/mDoc.
 - Trust models: we conducted an extensive analysis of three different models including [OpenID Federation](#), [EBSI](#) and [TRAIN](#). As a result, we concretely identified their trade-offs between security, interoperability and practicability. We are currently leaning towards EBSI and OpenID Federation models in our SSI development.
 - Cryptographic storage and operations: we are prototyping the use of Bull Proteccio CC EAL 4+ certified Hardware Security Module.

3.3.6.4 EXPLOITATION PLAN SUMMARY

Atos is a global leader in digital transformation with c. 92,000 employees and annual revenue of c. € 10 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The purpose of Atos is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

Eviden is an Atos Group company with an annual revenue of c. € 5 billion. Eviden is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 47,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come.

BDS is a specialized division in Eviden that brings together expertise in Big Data, Cybersecurity and Mission-Critical Systems. It holds the distinction of being the #1 player in Europe and #3 on a global scale in the field of Supercomputing, a significant achievement that showcases its leadership position in Europe and its strong presence and competitiveness in the worldwide market. The division relies on R&D teams whose expertise is recognized internationally and strongly contributes to the development of Eviden technology portfolio, from infrastructures to smart data platforms and industry solutions.

The results from SAFE6G will play a vital role in boosting the innovation process within the organisation. In SAFE6G, the BDS team plays two main roles, the first one leading the development of a framework to support and ease the development and execution of AI/ML algorithms across multiple domains; the second one as contributor on security and privacy aspects through the exploration of an identity management system allowing users to have control over their data.

In this context, the team foresees the following exploitation scenarios as the most suitable for its Key Exploitable Result, that will be further explored during the project lifetime:

- **Knowledge transfer:** The team will make sure that the knowledge acquired during its participation in the project is transferred, both internally and externally.
- **Technology Transfer:** Whenever possible, the team will promote that the technical outcomes of the project are reused.
- **Integration in research projects:** Participation in new research projects where the technical outcomes of the project can be presented as background IP contribution.
- **Enhancement of the Eviden portfolio:** The knowledge and the expertise acquired during our participation in the project and, whenever possible, the resulting technical outcomes will be used for evolving the BDS portfolio via the internal promotion of knowledge / technology transfer.

<i>Innovation To be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
MLOps Framework	Eviden Further research, enhancement of Eviden portfolio, consultancy services	C: IBM, Google, AWS S: Scalable AI integration W: Production-readiness challenges R: Market adoption uncertainty	TBD	TBD	AI-driven networks, enterprise ML solutions	TBD

SSI System	Eviden	Digital identity services, cybersecurity solutions	C: Decentralized ID providers S: Compliance with EU regulations W: Standardization challenges R: Competition with blockchain SSI platforms	TBD	TBD	Telecom, Banking, Education	TBD
-------------------	--------	--	---	-----	-----	-----------------------------	-----

Table 10: Summary of Exploitable Results (Eviden)

3.3.7 UNIWA EXPLOITATION PLAN

The University of West Attica (UNIWA), a pivotal partner in the SAFE-6G project, contributes its expertise in computational resources and reliability functions. Leveraging its advanced cloud and high-performance computing (HPC) infrastructure, UNIWA provides essential capabilities for training machine learning models and ensuring system’s reliability in next-generation 5G/6G networks. Below is a detailed outline of UNIWA’s contributions, forming the foundation for its exploitation strategy.

3.3.7.1 BACKGROUND CONTRIBUTIONS

UNIWA provides its cloud and HPC infrastructure as a background contribution, enabling advanced computational capabilities for SAFE-6G.

1. Cloud Computing Infrastructure

- Platforms include OpenStack, Kubernetes (K8s) and Docker for scalable deployment and orchestration.

2. HPC Infrastructure

- GPU-enabled systems for high-performance computation using Kubernetes and Docker.

Implementation Limitations

- Access to computational resources is controlled and granted through secure encrypted tunnels (VPN).

Exploitation Limitations

- Access rights are governed by the Consortium Agreement and exclude commercial use.

These contributions provide the computational foundation for developing and testing innovative security and reliability functions within SAFE-6G.

3.3.7.2 FOREGROUND CONTRIBUTIONS

UNIWA is developing the **Reliability Application** as its key contribution to the SAFE-6G project.

Asset #1

- **Asset Name:** Reliability Application
- **Asset Type:** Security Function
- **Description:**
 - A network application (NetApp) that serves as a security function within SAFE-6G to ensure the required **Level of Trust (LoT)**.

- Collects data from virtual, computational and network resources to feed the **SAFE-6G Cognitive Coordinator's AI agent**.
- Trains **ML models** locally to predict performance metrics under varying operational conditions.
- Optimizes decisions for configurations and policies to maintain **reliability**, avoiding system-breaking points such as **maximum resource utilization**.
- **Availability:**
 - Code will be made available through the SAFE-6G GitLab repository.
- **Protection:**
 - The first version of the **Reliability Application** will be released as open source.
- **Exploitation Limitations:**
 - Dissemination and exploitation require consent from the intellectual authors.
- **Status:** 40% complete.

Strategic Goals

Through its contributions to SAFE-6G, UNIWA aims to:

- Enhance **reliability in 5G/6G networks** through advanced ML-driven security functions.
- Validate the **Reliability Application** in real-world scenarios using SAFE-6G infrastructure and open-access datasets.
- Promote **adoption of its innovations** by releasing the initial version as **open-source**, fostering collaboration and further development.

3.3.7.3 EXPLOITATION STRATEGY AND MARKET OPPORTUNITIES

UNIWA will leverage SAFE-6 G's expertise in AI, machine learning and data analysis to develop a mature solution on the Reliability function aiming to build trustworthiness to communication networks in 6G industrial and educational domains.

SAFE-6G approach provides an innovative solution that focuses on creating a trust-centric 6G framework with innovative solutions in security, privacy and reliability. The project emphasizes integrating AI and ML to achieve high-performance, secure and user-centric communication networks. This approach unlocks several promising business opportunities in both industrial and consumer markets. Some key business opportunities are related to:

- Industrial and educational metaverse applications
- AI-enhanced security, privacy and resilience
- User-centric zero-touch orchestration
- Explainable AI solutions for 6G Networks

Marketable Products and Services

UNIWA aims to provide a **mature AI-enabled Reliability Function** in two versions:

- A basic version offered under an open-source license
- A customized version offered as a service, tailored to specific customer requirements

These offerings ensure widespread adoption in **research, enterprise security and AI-driven network reliability solutions**.

Path to Market

UNIWA as a research and educational organization aims to research and provide new knowledge to the students and communication engineers. So, the research outcome will be integrated into the curricula of the Depts. of Informatics and Computer Engineering and Electric and Electronic Engineering. However, additional paths will be investigated

- the establishment of a start-up company to commercialize the results
- the development of certification programs for professionals and students in AI applications for Reliability
- the organization of tailor-made training workshops for industry partners fostering ecosystem collaboration.

Near-Term Applications

At this point, the results of the SAFE-6G are in the development phase and the TRL level is still low. At the end of the project, we expect the SAFE-6G platform to be evaluated and verified in order to become a base for a more mature solution.

Current Market Position

UNIWA optimal resource orchestration solutions that can apply to domains of the cloud continuum, the next-generation networks. UNIWA currently works on the definition of relevant use cases that meet the needs of the market segments and collaborates with industry partners to estimate the market size and revenue potential.

UNIWA, as a university, focuses on research, design and development of state-of-the-art solutions with low TRL. UNIWA participates in several national and European research projects in the domains of next-generation networks, IoT, cloud/edge computing, etc.

While UNIWA does not have direct **commercial market share**, its contributions **drive innovation and future commercialization pathways** through research and spin-off initiatives.

Organization's Roadmap:

UNIWA aims to design the Reliability function following the cloud-native paradigm so it can be used as a stand-alone solution or as an easily integrated plugin. After the end of the project, the Reliability function will be a TRL 8 solution.

SAFE-6G tasks and fields align with the roadmap of the UNIWA research team, as our research interests are identical.

Technologies and Work Packages:

UNIWA focuses on the development of the Reliability function (WP4) and on the validation and evaluation of the SAFE-6G platform (WP5).

3.3.7.4 EXPLOITATION PLAN SUMMARY

UNIWA’s exploitation strategy focuses on developing the Reliability Function as an AI-powered trust and security application for next-generation networks. By leveraging SAFE-6G’s AI, ML and data analytics capabilities, UNIWA aims to build trustworthiness in 6G networks, particularly in industrial and educational domains. The short-term objective is to validate and optimize the Reliability Function, integrating it into SAFE-6G’s Cognitive Coordinator AI framework. The long-term objective is to offer a modular, AI-driven reliability solution for cloud-native, user-centric 6G networks.

Key strategic actions include:

1. Open-source release of the basic Reliability Function to encourage collaboration and adoption.
2. Industry engagement through training and certification programs to enhance commercial viability.
3. Integration into university curricula and future research projects to expand knowledge transfer.
4. Exploration of start-up and licensing opportunities for commercialization beyond SAFE-6G.

By combining AI-driven security, network reliability optimization and cloud-native orchestration, UNIWA ensures that its contributions remain at the forefront of trust-based 6G innovations.

<i>Innovation</i>	<i>To be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
Reliability Function	UNIWA	Open-source software and commercial services	Competition: Other AI-driven reliability solutions for 5G/6G URLLC. Strengths: AI-enhanced performance prediction and network optimization. Weaknesses: Currently at low TRL. Risks: Rapid technological advancements in 6G may outpace development.	No conflicts	3 years	AI-driven network orchestration, zero-touch security	Not yet determined

Table 11: Summary of Exploitable Results (UNIWA)

This exploitation plan ensures that UNIWA’s Reliability Function contributes to next-generation AI-driven network security and trust solutions while aligning with broader SAFE-6G objectives.

3.3.8 SPACE HELLAS EXPLOITATION PLAN

SPACE, a key partner in the SAFE-6G project, is developing innovative solutions for enhancing privacy in 6G networks. With its extensive expertise in privacy and security, SPACE is building its contributions from the ground up to ensure that privacy is embedded by design in the SAFE-6G framework. This exploitation plan outlines SPACE’s contributions, strategic goals and commercialization pathways.

3.3.8.1 BACKGROUND CONTRIBUTIONS

SPACE does not require any specific background contribution for its activities in SAFE-6G. All work begins from scratch, ensuring a privacy-by-design approach tailored specifically to 6G network requirements.

- **Background Status:**
 - No background technologies or assets are introduced for project use.
 - SPACE relies on its in-house expertise in privacy and security.
- **Implementation and Exploitation Limitations:**
 - No specific limitations are outlined for background contributions.

By developing its technology from the ground up, SPACE ensures that its contributions align seamlessly with SAFE-6G's objectives.

3.3.8.2 FOREGROUND CONTRIBUTIONS

SPACE is developing the Privacy Function, a key component in the SAFE-6G project.

Asset# 1

- **Asset Name:** Privacy Function
- **Asset Type:** Platform Component – Trust Function
- **Description:**
 - The Privacy Function leverages an AI-powered Decision Support System (DSS) to enhance service privacy in both pre-deployment and post-deployment stages.
 - Analyzes privacy requirements and risks to provide tailored recommendations, enhancing the Level of Privacy (LoP).
 - Ensures privacy by design, safeguarding user data and enhancing trustworthiness in 6G networks.
- **Availability:**
 - The Privacy Function will be released under a free, permissive license, ensuring accessibility for consortium partners and external stakeholders.
- **Protection:**
 - The solution will remain open access, maximizing its impact through wide dissemination.
- **Exploitation Limitations:**
 - No limitations at this stage, but ownership of the results remains with SPACE and Consortium Agreement provisions must be respected.
- **Status:** 30% complete.

Strategic Goals

SPACE aims to:

- Enhance privacy in next-generation networks by integrating privacy-by-design principles into SAFE-6G.
- Validate the Privacy Function through real-world 6G scenarios using the SAFE-6G infrastructure.
- Promote wide adoption of the Privacy Function by offering it under a free, permissive license.

3.3.8.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

Business Opportunities

- Commercializing the User-Centric Privacy Function, integrating it into SPACE's existing commercial offerings to address growing privacy concerns.
- Building strategic partnerships with other industry players and research entities.
- Enhancing SPACE's cybersecurity and privacy portfolio by integrating AI-powered privacy control for next-generation networks.

Marketable Products and Services

The User-Centric Privacy Function will be a standalone privacy enhancement for 6G services, ensuring that data security and privacy remain at the core of future networks.

- **Key Benefits:**
 - Provides privacy control to users.
 - Compatible with SAFE-6G's broader security framework.
 - Supports future 6G privacy standards and regulations.

Path to Market

A structured approach will be followed for commercialization:

1. Development of Proof of Concept (PoC) for the Privacy Function.
2. Integration into the SAFE-6G framework to assess performance.
3. Testing and validation in project use cases.
4. Further development to enhance TRL (Technology Readiness Level).
5. Alignment with upcoming 6G privacy regulations.
6. Commercial deployment via early adopters and scaling up.

Near-Term Applications

- The Privacy Function will be tested in the SAFE-6G pilot use cases.

Total Addressable Market (TAM)

No tangible estimation. The global 6G market is expected to reach US\$ 5.23 billion by 2031; it is expected to register a CAGR of 32.1% during 2025–2031. Given the increasing emphasis on data privacy and security, it is reasonable to anticipate that a substantial portion of the 6G market will be dedicated to privacy-preserving related technologies.

Current Market Position

Space Hellas is the leading Digital Integrator and Service Provider in South Europe, demonstrating strong partnerships with Global IT companies such as SAP, Microsoft, CISCO, IBM etc., focusing on verticals (i.e. Telcos, Financial Inst., Health Sector, Retail, Fuel, Energy, FMCG, Manufacturing, Services) for both commercial and defense applications to private and public clients.

Organization’s Roadmap

SAFE-6G roadmap is fully aligned with the roadmap of the company for the specific work. The targeted TRL by the end of the project is 4, so further actions are foreseen in the short-term & long-term towards its commercial deployment.

SAFE-6G roadmap is fully aligned with the roadmap of the company for the specific work, as this function is a new concept/potential product for the company and the project roadmap was adopted for its development.

Technologies and Work Packages

The technology being developed is the user-centric privacy function. The main work is done under WP4, T4.4 while associations exist with WP2 (requirements/ architecture and KPIs) as well as with WP5 (integration, validation, pilots).

Current State of the Art

In 6G privacy, state-of-the-art research focuses on user-centric privacy frameworks, differential privacy, federated learning and homomorphic encryption to protect user data. Current approaches include privacy-aware AI models for adaptive data sharing, network slicing with customizable privacy levels and blockchain-based identity management to ensure decentralized, transparent and user-controlled privacy.

Competitors

More and more organizations are working on addressing privacy concerns in the 5G and beyond networks, such as Nokia, Huawei, other similar to SAFE-6G collaborative projects (i.e. ENSURE-6G) etc.

3.3.8.4 EXPLOITATION PLAN SUMMARY

The exploitation plan for the user-centric privacy function in the SAFE-6G project focuses on commercializing and integrating the solution into B5G networks while ensuring compliance with the evolving regulatory landscape. Key activity is the development of a PoC and testing its effectiveness through the project use cases. Also, alignment with future 6G specific standards is foreseen. The function will be positioned as a privacy enhancement for 6G services where data privacy & security are critical and collaborations will be sought to accelerate the deployment in the market and increase adoption of the solution.

<i>Innovation</i>	<i>To be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
Privacy Function	SPACE	Further development to increase	C: Growing competition from major privacy-focused	No conflicts	TBD	6G networks, cybersecurity	TBD

		<p>TRL, with the aim of integrating into commercial offerings</p>	<p>organizations (e.g., Nokia, Huawei, ENSURE-6G). S: Provides user control over privacy, integrates with other SAFE-6G security components, supports 6G compliance. W: Function is not commercially ready yet. R: Unstable regulatory landscape, evolving privacy/security threats.</p>			<p>ty providers, enterprise privacy solutions</p>
--	--	---	--	--	--	--

Table 12: Summary of Exploitable Results (SPACE)

This plan ensures SPACE’s Privacy Function becomes a market-ready privacy enhancement for 6G services, offering AI-driven privacy control to users while complying with future 6G standards and security frameworks.

3.3.9 INFOLYSIS EXPLOITATION PLAN

INFOLYSIS, a key partner in the SAFE-6G project, specializes in advanced conversational AI, chatbot technologies and IoT integration tools to improve user interaction and operational efficiency in 5G/6G networks. With a strong focus on intent-driven applications and generative AI, INFOLYSIS is developing solutions that streamline interactions, enhance automation and facilitate trustworthy AI-enabled network functions.

The following exploitation plan details INFOLYSIS’s contributions and strategic approach for commercializing and leveraging project outcomes within enterprise, industrial IoT and telecommunications markets.

3.3.9.1 BACKGROUND CONTRIBUTIONS

INFOLYSIS provides a range of commercially available services and products as its background contribution, focusing on intent-driven conversational AI and IoT integration:

1. **Intent-Driven Chatbots:**
 - Chatbots enriched with deep learning (DL), natural language processing (NLP) and generative AI technologies/models.
2. **Customizable Chatbot Platforms:**
 - Platforms for creating bespoke conversational chatbots, statistical dashboards and targeted messaging.
3. **Indoor Localization Features:**
 - Chatbots enhanced with indoor localization capabilities for precise maintenance in complex environments.
4. **IoT Virtual Gateways and VNFs:**
 - Virtual Network Functions (VNFs) for IoT protocols mapping and interoperability in 5G/6G environments.

Implementation & Limitations:

- The background technologies will be used "as is" solely for the project's purposes and in their commercially available form.
- Ownership remains with INFOLYSIS and no source code is provided.
- Access rights to these technologies (or their further developed versions) for exploitation will require a formalized exploitation agreement with fair and reasonable financial terms and royalties.

By providing and further developing these commercial AI and chatbot solutions, INFOLYSIS supports SAFE-6G's objectives while protecting its proprietary assets.

3.3.9.2 FOREGROUND CONTRIBUTIONS

INFOLYSIS is developing the "INFOLYSIS SAFE-6G Chatbot" application as a key SAFE-6G innovation. The INFOLYSIS SAFE-6G chatbot, which captures the user's intent and translates free-text requests into structured LoTw parameters for the network application. The INFOLYSIS SAFE-6G chatbot offers a natural language-based interface so that non-experts can request advanced network services without the need of learning technical details.

Asset#1

- **Asset Name:** Chatbot
- **Asset Type:** Application
- **Description:**
 - Facilitates user interaction by interpreting input, analyzing intent and matching responses to five distinct functions.
 - Supports structured understanding and processing of user requirements, enhancing the clarity and efficiency of interactions.
 - Designed to classify user input for further processing, ensuring each function is supported with clear, actionable responses.
- **Availability:**
 - Delivered as a web application accessible through a browser interface, ensuring ease of use for consortium members and external stakeholders.
- **Protection:**
 - No actions have been planned for intellectual property protection at this stage. The asset is part of INFOLYSIS's commercial offerings and no source code will be provided.
- **Exploitation Limitations:**
 - Access to the chatbot and related INFOLYSIS background for exploitation requires a signed exploitation agreement with fair and reasonable financial terms and royalties.
- **Status:** Development is 20% complete.

Strategic Goals

INFOLYSIS aims to:

- Advance conversational AI and intent-driven interaction technologies in 5G/6G environments.
- Validate its chatbot solutions in real-world applications, leveraging the SAFE-6G infrastructure.

- Establish clear pathways for commercialization while aligning with its existing product portfolio and licensing model.

3.3.9.3 EXPLOITATION STRATEGY AND MARKET OPPORTUNITIES

INFOLYSIS plans to support the future of 5G/6G networks with its innovative AI, IoT/continuum integration and chatbot technologies. The standout exploitation opportunity lies in **intent-driven AI** chatbots, which have potential to transform user interaction in various fields such as smart cities, autonomous vehicles and enterprise-level systems. By leveraging SAFE-6G's infrastructure, INFOLYSIS could refine these applications for large-scale deployment and commercial exploitation within the field of security and trustworthiness too.

Business Opportunities:

- Enhanced operational efficiency in 5G/6G networks through AI-powered interaction platforms.
- IoT integration tools for next-gen industries requiring seamless and trustworthy device interoperability.
- Advance conversational AI and intent-driven interaction technologies in 5G/6G environments.
- Validate its chatbot solutions in real-world applications, leveraging the SAFE-6G infrastructure.
- Licensing and commercializing intent-driven chatbots for enterprise applications.

Marketable Products and Services

Intent-Driven Chatbots: A key product emerging from SAFE-6G is a chatbot platform, with deep learning and NLP capabilities tailored to 5G/6G environments. This can be marketed as a standalone product or integrated into enterprise platforms (with focus on trustworthiness aspects too).

Path to Market

- Demonstrating solutions via SAFE-6G pilot deployments.
- Establishing strategic partnerships with network providers.

Intermediate steps: Achieving certifications and aligning with emerging 6G standards.

Near-Term Applications

Intent-Driven Chatbots: Suitable for customer support and enterprise systems. These could be deployed in fields like industries and telecommunications for immediate use cases, such as interactive assistants or predictive maintenance.

Total Addressable Market (TAM)

Initially the European markets of the related SAFE-6G use cases are targeted to be addressed, expanding later to new fields and larger market sizes (from the research and experimentation level, to an entry level commercial applicability).

Current Market Position

Market presence in the field of chatbot applications with commercial presence in the fields of retailing, marketing, tourism, education and maritime. In parallel, new market opportunities are searched through R&D activities in the fields of ICT ecosystem, 5G/6G technologies, IoT, DL/NLP and NTN.

Impact on Business Performance

The exploitation of AI-driven solutions for 5G/6G networks, coupled with chatbot apps, could significantly increase INFOLYSIS's revenue and gross margin, driven by collaborations in telecoms and enterprise markets.

Organization's Roadmap

- 2024-2026: Finalize SAFE-6G chatbot development and deploy/test it within the related pilot use cases.
- 2027-2029: Scaling via potential exploitation/commercialisation initiatives for introducing the SAFE-6G related chatbot product/service to new markets, addressing existing needs.
- 2029+: Expand offerings to more related markets like smart cities.

Alignment with Roadmap

The goals in SAFE-6G align with INFOLYSIS's roadmap, focusing on AI and IoT/continuum integration for ensuring the desired levels of Trust in business applications and processes. The chatbot application, an important output of the project, couples well with related enterprise solutions providing additional focus on aspects such as security and trustworthiness.

Technologies and Work Packages

Implementation of intent-driven AI chatbots and advanced AI models, integrated with robust security functions to ensure reliable and secure user interactions. These technologies contribute to the generation of accurate trust level recommendations. (*Work Packages: WP3, WP5*).

Competitors

- **Market Areas:** Telecommunications, customer service automation and industrial IoT.
- **Key Features:** Conversational AI platforms, cloud-based chatbot solutions and IoT network solutions.
- **Overcoming Competition:** INFOLYSIS would need to enhance its real-time intent processing capabilities and scalability to surpass potential competitors.
- **SAFE-6G Advantage:** Through real-world testing and integration into 5G/6G networks, INFOLYSIS's solutions will offer unique differentiation in terms of network-specific AI and IoT functionalities.

Leading players include **Google AI, Amazon Web Services (AWS)** and **IBM Watson**.

Standards

- **Controlling Body:** Standards are overseen by organizations like 3GPP and ETSI.
- **Impact on Commercial Uptake:** Adherence to these standards will ensure wider adoption and integration of INFOLYSIS’s technologies within established 5G/6G frameworks.

Publications and IP

Publications/IP: INFOLYSIS has already released and will release papers related to its AI chatbot platforms and IoT integration, potentially securing potential IP rights in conversational AI or IoT interoperability. No further actions have been planned for intellectual property protection at this stage. The asset is part of INFOLYSIS’s commercial offerings, and no source code will be provided.

Application Environment Changes

The evolving telecom landscape and accelerating adoption of 5G/6G networks will drive demand for technologies like INFOLYSIS's chatbot solutions and IoT gateways.

Opportunities and Threats

- **Opportunities:** Exploiting the fast-evolving 5G/6G market could lead to high growth for conversational AI and IoT-based applications.
- **Threats:** Rapid technological changes and competition from established AI and IoT giants could challenge market penetration and actual customers’ needs.

3.3.9.4 EXPLOITATION PLAN SUMMARY

INFOLYSIS will exploit SAFE-6G results by increasing INFOLYSIS’s presence and penetration in the respective areas of research and will facilitate the processes to make the project achieve maximum visibility and to maximize its impact within the business and scientific communities, to guarantee a fast adoption of the project outputs and easier commercialization of its services.

INFOLYSIS participation to the SAFE-6G project in conjunction with the participation and outcomes of relevant projects (such as EVOLVED-5G, SECANT, aerOS) will further enrich the know-how and the research expertise of the company in chatbot and AI related technologies that can further foster its R&D activities.

In specific, INFOLYSIS intends to leverage the SAFE-6G project outcomes to enhance its chatbot solutions further. By incorporating new technologies and insights gained during the project, in parallel, INFOLYSIS aims to offer more sophisticated and context-aware chatbot services, improving customer engagement and operational efficiency for clients across various sectors.

INFOLYSIS will also exploit SAFE-6G results within scientific communities by intense communication and dissemination of project's activities and achievements.

<i>Innovation</i>	<i>To be Exploited By</i>	<i>Type of Exploitation</i>	<i>of Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
-------------------	---------------------------	-----------------------------	---	-----------------------	-----------------------	------------------------	---------------------

AI Intent-Driven Chatbot App	INFOLYSIS	Product/Service	C: Major AI chatbot platforms (Google AI, AWS, IBM Watson). S: Tailored for 5G/6G networks , integrates intent-driven automation . W: Function still requires validation and scalability testing. R: Rapid changes in AI technology could impact deployment.	None	3+ years	Telecom, industrial IoT, smart automation	>25%
-------------------------------------	-----------	-----------------	--	------	----------	--	----------------

Table 13: Summary of Exploitable Results (INFOLYSIS)

INFOLYSIS is poised to leverage SAFE-6G AI advancements to drive conversational AI in future networks, ensuring scalable, automated and secure chatbot solutions for enterprise adoption.

3.3.10 EBOS EXPLOITATION PLAN

EBOS, a key partner in the SAFE-6G project, contributes advanced patented technologies aimed at enhancing security, privacy and trustworthiness in next-generation networks. Combining its expertise in software-defined perimeters (SDPs) with innovations developed during the project, EBOS aims to address critical challenges in network safety and microservice protection. Below is a detailed description of its contributions, which form the foundation for its exploitation strategy.

3.3.10.1 BACKGROUND CONTRIBUTIONS

EBOS provides two critical patented technologies as part of its background contribution:

1. **Software Defined Perimeter Integration for Software-Defined Cellular Telecommunications Networks**
 - **Description:** Integrates an SDP into 5G/6G telecommunications networks to enhance security and ensure privacy and trustworthiness.
2. **Dynamic Reconstitution of an SDP for Microservices Network Applications in a 5G/6G Network**
 - **Description:** Provides dynamic reconstitution capabilities for SDPs to support secure microservice applications.
- **Implementation & Exploitation Limitations:**
 - The background technology is to be used exclusively within the boundaries of the SAFE-6G project for research purposes.
 - The technology is patented and owned by EBOS and its use beyond the project requires specific agreements.
 - Any exploitation outside the project requires a signed exploitation agreement that defines licenses and royalties.
 - Only organizations or companies with access to their own core can exploit the developed function.

Through these contributions, EBOS provides foundational technologies to enhance safety, security and privacy in next-generation networks.

3.3.10.2 FOREGROUND CONTRIBUTIONS

As part of its involvement in SAFE-6G, EBOS is developing a modified version of an Integrated SDP for network services as part of a Safety Function to enable enhanced network safety and microservice protection.

Asset#1

- **Asset Name:** Integrated Software-Defined Perimeter (SDP)
- **Asset Type:** Network Function
- **Description:**
 - The SDP technology integrates into the 6G infrastructure (User-Centric 6G Packet Core) to independently create perimeters around network services. These perimeters are tailored to individual users, ensuring access only to requested features and services while limiting exposure to the rest of the network. Enables micro-fragmentation and granular authentication to mitigate safety threats, creating a user-centric and secure network environment.
- **Availability:**
 - The SDP will be containerized and deployed as part of the overall SAFE-6G solution, interacting with the core network.
- **Protection:**
 - The technology is protected under a granted patent.
- **Exploitation Limitations:**
 - The technology is protected under a granted patent.
- **Status:** 15% complete.

Strategic Goals

EBOS aims to:

- Advance the state of security, privacy and trustworthiness in next-generation networks through patented SDP technologies.
- Validate its solutions in real-world scenarios in collaboration with SAFE-6G partners.
- Establish commercialization pathways that ensure alignment with its patents and licensing models.

3.3.10.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

eBOS focus in the SAFE-6G project is located on the development of a SDP that will be integrated within the proposed user-centric 6G Packet Core. The perimeter as a feature will provide strong network security and safety, reassuring the protection of infrastructure nodes and the availability of relevant microservices to specific users. A standout exploitation opportunity is the seamless integration of the SDP stack with the UPF and AMF, initiating the SDP controller to establish a VPN connection for mutual authentication with the UE. This creates a secure and personalized network.

Business Opportunities

- Enhanced security solutions for telecommunication networks.
- Development of user-centric, case-specific, network safety services.
- Providing robust infrastructure protection for 6G networks and nodes.

Marketable Products and Services

The **SDP framework** developed in SAFE-6G will be marketed as:

- SDP solutions integrated within 6G networks.
- Advanced VPN solutions for secure user authentication.
- Customized microservices for user-specific applications.
- Infrastructure protection services for telecommunication providers.

These products could fit within eBOS' current portfolio of software suites provided to our customers as add-ons, but they also bear the potential of a new range of network safety solutions that will promote eBOS' position in the market of 5G and 6G cyber security.

Path to Market

The main foreseeable steps to the market are:

- Conduct Market Analysis Research
- Define the total Addressable Market
- Identify business opportunities
- Assess the Expected Market Impact
- The development of Near-Term Applications

Near-Term Applications

- Secure network perimeters for critical infrastructure.
- Enhanced mobile network security for enterprises and government agencies.
- Deployment of user-specific security microservices in 6G environments.

Total Addressable Market (TAM)

The target audience of our solution includes Mobile Network Operators (MNOs), Telecom vendors, Tier-1 suppliers, Security service providers (SMEs), ICT application providers (SMEs), Research and Technology Organisations (RTOs), SDOs with key locations in North America, Europe and Asia. The market size is expected to grow significantly with the adoption of 6G technologies.

The market for SDP applications in 5G networks is experiencing significant growth. As of 2023, the global SDP market was valued at approximately USD 6.92 billion and is projected to reach USD 8.62 billion in 2024[9] [9]. The market is expected to continue expanding, with forecasts suggesting it could reach USD 50.97 billion by 2032, growing at a compound annual growth rate (CAGR) of 24.9% during the forecast period[9].

This growth is driven by:

- the increasing need for secure remote access,

- the adoption of cloud services,
- the proliferation of IoT devices,
- The rise in remote work, accelerated by the COVID-19 pandemic[9] .

Regional Insights

- Europe: As Cyprus is a member of the EU with advanced industrial and cyber market, Europe is the natural target market for its products and services.
- North America: This region currently holds the largest market share due to its advanced technological infrastructure and high adoption rates among large enterprises
- Asia Pacific: Expected to exhibit the fastest growth rate, driven by increasing investments in digital security across various industries, including telecommunications and finance[9] . **¡Error! No se encuentra el origen de la referencia.**

Current Market Position

eBOS is solidifying its position as a significant player in the R&D sector, particularly within the European Union's Horizon Europe framework, recognized as one among the top 10 SMEs in Europe for its ambitious and competitive participation in Horizon Europe projects. The company has successfully secured funding for multiple EU-funded projects, including those under the European Defence Fund, which highlights its innovative capabilities and commitment to technological excellence.

eBOS's involvement in various cutting-edge projects, such as those focusing on 6G research, cybersecurity and sustainable technologies, further underscores its strong market position and influence in driving technological advancements. This strategic engagement in high-profile projects and collaborations with key industry partners positions eBOS as a key innovator and leader in the field.

Impact on Business Performance

The innovations driven by the project are expected to positively impact gross margin and net profit by expanding our product offerings and entering new markets reflecting a 10% increase in revenue is expected within 2 years after the project's completion.

Organization's Roadmap

- Q1 2027: Completion of pilot projects and initial market launch.
- Q3 2027: Expansion of product offerings and market reach.
- Q1 2028: Full-scale deployment and continuous improvement.

eBOS' targeted fields and tasks in SAFE-6G align with our roadmap by focusing on user-centric network security solutions and leading the innovations for the creation of a SDP that will be directly integrated into the systems core.

Technologies and Work packages

eBOS is the task leader of Task 4.2 User-Centric Safety function. The objective of this task is to design and develop an open-source SDP stack that emphasizes strong network security and safety, tailored to function seamlessly with SAFE-6G's proposed user-centric 6G Packet Core. The developed SDP will provide the protection of infrastructure nodes and ensuring the availability of relevant microservices to specific users, creating new opportunities and capabilities for the telecommunication industry. Specifically, the SDP stack will be integrated with the UPF, the AMF initiating the SDP controller, which will establish a VPN connection for mutual authentication with the UE. Upon successful authentication of the UE with the controller and the authentication host, a perimeter will be established for the user, which will contain all the necessary components. Additionally, microservices on the User Plane will be independently authenticated before being added to individual perimeters and deployed to the network.

Current State of the Art

eBOS already holds a granted patent for an SDP based software solution in 5G networks. As a member of SAFE-6G, eBOS has proceeded to the development of such a perimeter that will be fully compatible with all the system's components.

Competitors

Leading companies in the field that could be potential competitors include companies like Cisco, Nokia and Ericsson that all operate in the fields of network security and telecommunication infrastructure. Key features of their offerings include advanced security protocols and scalable network solutions. For the solution developed within SAFE-6G to be competitive to what is offered by its potential competitors, it is imperative that its marketable version, to focus on user-centric action and seamless integration with 6G technologies. SAFE-6G reinforces our competitive advantages by providing a unique, user-focused security framework.

Standards

Proposed standards for our technology area include those set by 3GPP and ETSI. These standards are overseen by bodies like the ITU and GSMA. Such bodies could impact the commercial uptake of SAFE-6G by ensuring interoperability and compliance with industry norms.

Environment Changes:

- **Increased IoT Adoption:** The rapid increase of IoT devices requires robust security measures, which aligns with SAFE-6G's focus on secure microservices and user-centric perimeters.
- **Edge Computing Growth:** The shift towards edge computing necessitates secure, low-latency connections, which SAFE-6G can provide through its SDP and VPN solutions.
- **Regulatory Changes:** Evolving data protection regulations (e.g., GDPR, CCPA) demand enhanced security protocols, which SAFE-6G aims to deliver.
- **5G to 6G Transition:** The ongoing transition from 5G to 6G networks will require advanced security frameworks, positioning SAFE-6G as a critical component in this evolution.

Opportunities and Threats

Opportunities

- **Market Expansion:** Growing demand for secure 5G and 6G networks presents a significant market opportunity.
- **Partnerships:** Collaborations with telecom providers and tech companies can enhance market reach and innovation.
- **Standardization Leadership:** Contributing to the development of industry standards can establish SAFE-6G as a leader in network security.

Threats:

- **Competitive Pressure:** Major players like Cisco and Nokia could pose significant competition.
- **Technological Advancements:** Rapid advancements in cyber threats require continuous innovation to stay ahead.
- **Regulatory Hurdles:** Compliance with diverse international regulations can be challenging and resource intensive.

3.3.10.4 EXPLOITATION PLAN SUMMARY

eBOS exploitation plan for SAFE-6G focuses on leveraging the proposed SDP integrated with a user-centric 6G Packet Core to enhance network security and safety. The standout opportunity lies in the seamless integration of the SDP stack with the UPF and AMF, initiating the SDP controller to establish a VPN connection for mutual authentication with the UE. This creates secure, personalized network perimeters for users, enhancing the overall security and efficiency of 6G networks.

Business Opportunities:

The proposed solution bears significant potential in offering enhanced security solutions for telecommunication networks, developing user-centric network services and providing robust infrastructure protection for 6G networks. These solutions can fit within eBOS' portfolio by enhancing our existing offerings and expanding into the 6G market and security sector.

Roadmap Alignment:

Our targeted fields and tasks within SAFE-6G are aligned with our long-term strategic roadmap, focusing on user-centric network security solutions and the development of advanced microservices for 6G networks. eBOS target is to strengthen its presence in technologies related to SDP integration, user-centric microservices and secure VPN solutions, which are associated with Work Packages WP3 and WP4.

Path to Market:

eBOS strategy to bring these innovations to market includes conducting pilot projects with key industry partners, obtaining necessary certifications and engaging in strategic partnerships. Intermediate steps will involve extensive testing, collection of user feedback and iterative improvements to refine our solutions.

Market Impact estimation:

Currently, the estimated total addressable market for our contributions encompasses the global telecommunication sector, with key regions including North America, Europe and Asia. Our contributions are anticipated to positively impact revenue, gross margin and net profit by expanding our product offerings and penetrating new markets. To verify these preliminary estimations, further and more in-depth studies will be implemented that will potentially include wide surveys of potential partners and market users.

Detailed Competitive Landscape Analysis:

Leading competitors in this domain include companies such as Cisco, Nokia and Ericsson. To surpass these competitors, eBOS will focus on user-centric innovations and seamless integration with 6G technologies. SAFE-6G reinforces our competitive advantages by providing a unique, user-focused security framework.

Near-Term Applications:

Immediate applications of SAFE-6G technology could encompass secure communication solutions for critical infrastructure, enhanced mobile network security for end-users and the deployment of user-specific microservices within 6G networks.

Standardization:

We adhere to standards set by 3GPP and ETSI, overseen by bodies such as the ITU and GSMA. Through our involvement in WG that provide feedback to such standardization bodies we aspire to contribute to the future standards that will shape 5G and 6G communications.

Environmental Changes:

Changes in the application environment, such as the increased demand for secure mobile networks and the proliferation of IoT devices, could significantly impact SAFE-6G objectives by driving the need for advanced security solutions. As a result, continuous market research will be conducted in order to adapt the system’s capabilities.

<i>Innovation</i>	<i>To be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, Risks</i>	<i>Conflicting IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
SDP (Integrated in Safety Function)	EBOS	Software	C: Competitors include Cisco, Nokia, Ericsson. S: Established market, patent-protected innovation, granular security. W: Lack of existing 5G user-centric security models. R: Regulatory hurdles, competitive pressure.	Patent Protected	2 years	MNOs, enterprises, cybersecurity firms	10% additional revenue within 2 years

Table 14: Summary of Exploitable Results (eBOS)

By leveraging its patented SDP within SAFE-6G, EBOS is poised to expand its market share in 6G security while ensuring long-term competitive differentiation.

3.3.11 UPV EXPLOITATION PLAN

The Polytechnic University of Valencia (UPV) plays a crucial role in the SAFE-6G project, contributing its expertise in orchestration and management of computing continuum infrastructures. Leveraging the **aerOS meta-operating system**, UPV provides foundational services for managing and monitoring distributed resources and enables integration with advanced virtualization and orchestration technologies. Below is a detailed outline of UPV's contributions and its exploitation strategy.

3.3.11.1 BACKGROUND CONTRIBUTION

UPV contributes the **aerOS meta-operating system** (meta-OS) as its background expertise:

Core Features:

- The aerOS runtime enables registration, management and monitoring of processing units called Infrastructure Elements (IE).
- Foundational services for coordination, organization and service management among Edge IoT devices and dispersed computer resources.
- Facilitates integration, administration and data congestion management for Edge IoT.
- **Implementation Limitations:**
 - The aerOS meta-OS can be used internally within the project, adhering to the provided code and tools.
- **Exploitation Limitations:**
 - The aerOS meta-OS will be open source, but licensing details for the overall package and modules are yet to be defined.
 - Until licensing is finalized, the meta-OS is restricted to internal project use.

Through these contributions, UPV provides critical infrastructure to support orchestration and service management in SAFE-6G.

3.3.11.2 FOREGROUND CONTRIBUTION

UPV is developing two key assets within the **SAFE-6G** project:

Asset #1

- **Asset Name** : LLO for Helm Charts (Low-Level Orchestration Service)
- **Asset Type**: Service
- **Description**:
 - A custom LLO service integrated with aerOS to deploy, update, or delete workloads on computing elements.
 - Operates via Docker images or Helm charts and interacts with virtualization technologies for workload execution requests.
- **Availability**: Open-source code and packages will be available in a public repository.
- **Protection**: Copyright and **open-source license** (to be decided).
- **Exploitation Limitations**:
 - Until licensing is finalized, the LLO service is restricted to project use.
 - Proper attribution to UPV is required for dissemination.
- **Status**: 90% complete.

Asset #2

- **Asset Name:** aerOS' Tailored Version for SAFE-6G (“aerOS-6G”)
- **Asset Type:** Building Block
- **Description:**
 - A tailored version of aerOS for SAFE-6G, designed to manage the computing continuum infrastructure.
 - Orchestrates services, facilitates data exchange and provides observability across computing resources.
- **Availability:** Open-source code and packages will be available in a public repository.
- **Protection:** Copyright and open-source license (to be decided).
- **Exploitation Limitations:**
 - Restricted to project use until licensing is defined.
 - Proper attribution to UPV and aerOS is required for dissemination.
- **Status:** 40% complete.

Strategic Goals

Through its contributions to **SAFE-6G**, UPV aims to:

- Advance orchestration and management solutions for distributed infrastructures.
- Validate the tailored aerOS version and LLO service in realistic 5G/6G scenarios.
- Promote adoption of aerOS components by releasing them as open-source under a permissive license once finalized.

3.3.11.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

UPV is represented by the SATRD lab, a research group of the Communications department. Belonging to an academic institution, the group aims at improving its technological proposition (i.e., aerOS meta-OS) by adapting it to the specific characteristics of 5G/6G, in terms of orchestrating and monitoring computing resources and services in distributed, heterogeneous ecosystems. The participation of UPV in SAFE-6G and other competitive research projects plays a key role in order to enhance (and increase the number of) the features offered by aerOS, promoting its awareness within relevant communities (e.g., research, SMEs, Industry, etc.) and easing its adoption once the platform is released as an open source, full-fledged solution. Succeeding in this endeavour would improve UPV’s position and relevance in the research and innovation ecosystem, widening its opportunities.

Business Opportunities:

The new generation of cellular technology is becoming increasingly open, distributed and complex, offering more advanced features for stakeholders, innovators and users but in turn opening new attack surfaces. SAFE-6G proposes a novel architecture and reference implementation to mitigate potential issues related to trustworthiness, not only related to security. Thus, the framework and the individual solutions (e.g., trust functions) have impact potential to be further exploited and being part of the evolution of the 6G era. From the UPV perspective, SAFE-6G brings the opportunity of adapting aerOS to the needs of a different ecosystem (5G and beyond instead of Next-Generation IoT) and with new partners, resulting very beneficial to:

- improve and extend its functionalities.
- gather relevant feedback.
- catch their attention for future collaboration. In the mid-term, aerOS could become an alternative to existing MANO propositions.

Marketable Products/Services

A tailored version of aerOS' (aerOS-6G) for managing the computing resources and services of 5G and beyond ecosystems is targeted. Specifically developed for the project, a Low-Level Orchestrator (LLO) for managing services locally in the form of Docker images or complete Helm charts has been implemented, which could be leveraged jointly with aerOS or by alternative meta-OSs (via API or with K8s-compliant, declarative manifests).

As an expert entity in (designing, developing, integrating and leveraging) Next-Generation IoT enablers, these products fits perfectly within its portfolio. Specifically, the developed LLO could be used in any vertical with virtualization capabilities managed by Docker and/or Kubernetes.

Path to Market

UPV's products will not be commercialised by the entity. The plan is to publish them in public repositories, with permissive Open-source licensing. The team in charge is in conversations with the Apache Foundation to adopt aerOS as part of their catalogue of solutions. Despite having identified two products, namely aerOS-6G platform and the new LLO, the focus will be on the platform as it has been identified as key for the entity (thus, the following sections will focus mostly on it).

Near-Term Applications

A full-fledged version of aerOS still needs further enhancements, validation and investments to move to upper TRL levels. Besides, the developed LLO, as a standalone, independent service has the potential to be adopted or leveraged fast by existing meta-OSs; still, since the cloud continuum orchestration data model is still in pre-standardization stages, interoperability issues may occur that would require integration efforts.

Total Addressable Market (TAM)

The products would fit in two markets: the cloud continuum and the telecom-specific service orchestration markets. According to available reports[9] , the cloud continuum market reached a size of US\$ 3.9 Billion in 2023, and it is expected to grow at a rate of 13.45% during the next 8 years period.

North America and Europe are the regions with larger shares, with the former dominating. Other regions from Asia pacific are also key locations.

Current Market Position:

UPV does not hold any position in the market, as its solutions are of low TRLs. In the European research and innovation field, UPV is one of the top entities, with a historic of coordination in previous (H2020 ICT-30-2015 INTER-IoT, H2020 ICT-56-2020 ASSIST-IoT), current (HORIZON-CL4-2021-DATA-01 aerOS) and recently-awarded (HORIZON-CL4-2024-DATA-01 O-CEI) competitive projects related to the

computing continuum, being the latter a strategic project funded by the European Commission in the continuum field.

Impact on Business Performance:

It is not possible to estimate it in the same manner than a company in the market. Having these products in the entity's portfolio opens the door to create new and solidify existing collaborations with other entities, in the form of invitations to proposals for competitive projects, participation via Open calls, or via contracts/subcontracting (e.g., for R&D activities, consultancy, etc.). The consolidation of UPV's position in the computing continuum research field positively affects to the size and stability of the personnel of the group involved.

Organization's Roadmap:

Being the cognitive framework, the foreseen main solution stemming from the project activities, UPV will not have the capability to commercialize it nor use it, as it is not intended to be operated by academic entities nor is actively involved in their development. Depending on if and how the after-project collaboration with partners is formalized, UPV aims at continuing it under different formulas, including definition and implementation of additional features for aerOS to support the cognitive framework (e.g., to gather and manage contextual data from the delocalized computing elements, to deploy the framework, to manage the lifecycle of the trust functions, etc.) and better adapt it to the 5G and beyond ecosystem:

- In orchestration capabilities
- In services communication
- In the data model

Thus, UPV's plan focuses on the evolution of aerOS-6G as an alternative to MANO for the increasingly complex B5G ecosystem, where the convergence with cloud, edge and IoT technologies is quickly advancing. To that end, the aerOS-6G roadmap is to have a TRL 7-8 solution by 2030, ready for the initial 6G deployments.

Alignment with Roadmap:

In SAFE-6G, UPV leads the task related to manage the infrastructure and the services lifecycles, while also leads the work package related to the adaptation and evolution of the technological elements "surrounding" the cognitive framework (i.e., core, CAPIF, MLOPs, DataOps, use cases...).

SAFE-6G is the first contact of aerOS with 5G and beyond technologies, being extremely valuable to gather feedback and implement the first essential features tailored to the telco ecosystem. While the streamline version of aerOS targets "pure" cloud continuum ecosystems, the version for SAFE-6G will thus differ, but still it will not a real alternative to MANO as more effort will be needed afterwards.

Technologies and Work Packages

UPV focuses on the tailoring of a meta-operating system for the computing continuum and B5G and the integration of Cloud Native technologies to support the management of metrics, logs, automatic service mesh and virtualized networking. These activities are concentrated in WP3.

Current State of the Art

While the concept of meta-operating system (Meta-OS) is old, its applicability to the computing continuum is very recent. In the 5G ecosystem, they have not been considered yet, due mainly to the fact that the virtualized infrastructure is relatively limited in number of localizations (with very powerful servers) and owned/managed by one operator - or subcontracted. The continuum offers the possibility of opening the computing, data and network fabrics to more devices in a secure way, regardless of their type (heterogeneity), location and ownership.

MANO is the current standard for managing the infrastructure and services lifecycle, with different alternatives available (e.g., OSM, ONAP, Tacker, proprietary solutions, etc.). The UPV team already presented a conference paper about its state of the art back in 2022: *“Evolution of MANO Towards the Cloud-Native Paradigm for the Edge Computing”*, by A. Fornes et al. Besides, while competing with the US in the cloud market is complex, Europe keeps a good position in the telco, edge and IoT ecosystems. The convergence of them also with cloud opens new possibilities but also adds complexity and security concerns that must be evaluated: this is where Meta-OS comes to play. The UPV team also published in 2023 a journal article about current state of the art and future directions in the field: *“Cloud-Native Workload Orchestration at the Edge: A Deployment Review and Future Directions”*, by R. Vaño et al.

The EC is channelling all recent research and innovation efforts in computing continuum and related technologies in the EUCloudEdgeIoT (EUCEI) initiative, being Meta-OS a key building block for it. In fact, a specific task force is working jointly with ISO/IEC SC41 to work on the standardization of some of involved aspects. Still, Meta-OS have not been thoroughly explored for the 5G/6G ecosystem, being SAFE-6G to the best of our knowledge the first research action exploring its integration.

Competitors

Since UPV is an academic entity, there are no competitors from a market perspective. Still, the involved group aims at remaining relevant at the research fields involved (management and orchestration of virtualized infrastructure and services). In summary, these would be MANO and (other) Meta-OS providers.

It is complicated to know the real status of alternative Meta-OS providers, since they are still under implementation (low TRL). Regarding MANO providers, their advantage comes from the fact that they already follow the related ETSI standards, therefore any Meta-OS that aims at providing similar features in the orchestration field will need to perform some needed integrations before becoming a real alternative. UPV wants aerOS to become an alternative in the mid-term, working in the mentioned needs and gaining an advantage by providing attractive features not available in current solutions. SAFE-6G precisely helps UPV to better identify the specific needs from the telco, thanks to the partners involved from the telco realm.

Standards

Some standards are or will be core part of the product, like those related to NGSI-LD (from ETSI CIM) for the data fabric, NFV or MANO (also from ETSI). Besides, the definition of the computing continuum is evolving, with standardization efforts channelled through the EUCEI community through ISO/IEC JTC 1/SC 41. While dedicated meta-OS standards are not yet available, they might become a reality soon.

Publications and IP

IP rights and licenses that may affect are those from the aerOS base code. Currently, they are under decision and have not been applied yet. In any case, UPV coordinates and leads the streamline project, therefore no issues are foreseen in the mid/long term as permissive rights and OSS licenses are expected to be applied.

Application Environment Changes

The meta-operating system paradigm for the computing continuum is fostered by the EC, however, thought for the IoT-edge-cloud ecosystem and not envisioned specifically for the 5G and beyond field. SAFE-6G is the first project exploring their applicability in this environment, as an alternative or complementary to MANO. Thus, this first step is key to assess its potential.

Opportunities and Threats

Currently, MANO systems are thought for 4G and 5G, in the sense that current designs and implementations do not consider from their conception the multi-ownership of resources nor the availability of large number of delocalized, virtualized computing infrastructures. Therefore, the opportunity is there. Still, there are some threats to bear in mind, like the evolution of competitive meta-OS that could be leveraged in the 5G and beyond realm and the need of further investment to tailor it to the needs and applicable standards.

3.3.11.4 EXPLOITATION PLAN SUMMARY

UPV is a public and dynamic academic institution that aims at enlarging its portfolio of successful projects and expects to make an impact in the 5G and beyond ecosystem. As main exploitation result stemming from its participation in SAFE-6G, UPV expects to introduce and test aerOS-6G as a software platform to manage and orchestrate both infrastructure and service lifecycle in the 6G ecosystem. Being an academic partner, exploitable aspects include (i) enhancing the knowledge of specific technological fields developed in the project, (ii) gaining expertise and know-how with regards to actual deployments, (iii) augmenting the volume of the research team and consolidating that number, (iv) exploring new research lines and (v) envisioning potential continuation of the research through market-oriented actions (like technology transfer, consulting actions, startups or spin-offs creation).

All in all, UPV aims at keeping its relevant position in the meta-OS ecosystem while exploring new opportunities in other realms, like now in 5G and 6G. Given the limited resources available in the project, aerOS-6G will not be ready to be exploited by MNOs once the project ends; still, UPV plans to have the IP strategy and base license/s in place. Particularly, UPV envisions a 5-year plan from to further adapt it to the expected needs for 6G orchestration, therefore the next steps include continue

looking for public funding opportunities and collaborations with relevant stakeholders (like TID) to integrate features from relevant standards, such as MANO. These opportunities will come primarily through the participation in competitive proposals in Horizon Europe and SNS calls.

<i>Innovation To be exploited by</i>	<i>Type of Exploitation</i>	<i>Competition, Strengths, Weaknesses, (C, S, W, R)</i>	<i>Conflicting IP</i>	<i>Time-to-market after project end</i>	<i>Targeted Market</i>	<i>Expected ROI</i>	
aerOS-6G	UPV	Open-source meta-operating system	C: MANO providers (OSM, ONAP). S: Large-scale orchestration features. W: Lacks telco-specific optimizations. R: Time to adoption.	None	3 years	Cloud-edge orchestration	No direct ROI, increased research impact

Table 15: Summary of Exploitable Results (UPV)

3.3.12 8BELLS EXPLOITATION PLAN

8BELLS, a leading Cypriot SME with recognized expertise in security and privacy technologies, plays a central role in the SAFE-6G project as both the Exploitation and Innovation Manager and a main technical contributor to the differential privacy mechanisms in MLOps. 8BELLS stands as a pioneering, independent high-tech SME, strategically located in Nicosia, Cyprus and Athens, Greece, with a proven track record in delivering advanced ICT, cybersecurity and defence-related solutions across Europe. With over €2.2 million in revenue (2023) and a multidisciplinary team of ~25 experts, 8BELLS is recognized for its cutting-edge innovation, demonstrated by its European Innovation Management Academy scores of 69% in innovation performance and 67% in digital innovation.

As the Exploitation and Innovation Manager in SAFE-6G, 8BELLS plays a dual role: steering the commercialization and IPR strategy of the consortium and leading the technical implementation of differential privacy in MLOps, ensuring privacy-preserving mechanisms for AI model training and inference in the 6G context.

3.3.12.1 BACKGROUND CONTRIBUTIONS

8BELLS joins the SAFE-6G project, bringing both strategic insight and technical expertise. In this role, the company will lead the Exploitation and Innovation Management (T6.4) efforts and act as the primary technical contributor responsible for integrating Differential Privacy into MLOps. Through these dual leadership responsibilities, 8BELLS is not only driving technological innovation but also actively shaping the project's broader societal value, market readiness and sustainable impact.

This significant contribution leverages 8BELLS's extensive experience in cybersecurity, privacy engineering, secure telecommunications systems and AI/ML orchestration. The company's capabilities are well-established through active involvement in over 10 prestigious European Defence Fund (EDF) projects and various Horizon Europe initiatives. Recognized by the European Innovation Management Academy for excellence in innovation and digital transformation, 8BELLS is uniquely positioned to

develop cutting-edge, privacy-focused technologies and lead their successful transition from innovation to market-ready solutions.

Technical Background - Differential Privacy

8BELLS's role in SAFE-6G is underpinned by years of dedicated development in AI, data privacy and secure communication systems, positioning it to successfully deliver a robust differential privacy framework for SAFE-6G's MLOps processes. The company's extensive expertise encompasses several critical domains:

- **Security and Privacy Engineering for Telecom and Defense:** 8BELLS has successfully implemented robust privacy architectures for private and governmental applications, including military-grade secure communications, access control systems and threat mitigation technologies. This expertise ensures practical and effective solutions for privacy-preserving AI in operational contexts.
- **AI/ML and Cognitive Function Integration:** The company's experience includes real-time threat detection, autonomous systems and predictive maintenance, demonstrating deep technical knowledge of neural network optimization, model interpretability and edge-cloud AI orchestration. These skills are crucial for successfully applying Differential Privacy (DP) in sophisticated MLOps environments.
- **Private Cloud and High-Performance Infrastructure:** Equipped with its own data center, HPC nodes, cloud orchestration frameworks like Kubernetes and telecom-grade 5G testbeds, 8BELLS can rigorously simulate and validate scalable, DP-enhanced MLOps workflows, ensuring high reliability and effectiveness.
- **Workload Orchestration and Data Lifecycle Management:** Proficiency in Kubernetes-based orchestration and containerized AI environments allows 8BELLS to design modular, scalable and privacy-compliant MLOps toolchains. This capability is essential for real-time deployment of advanced DP techniques such as noise injection, data perturbation, gradient clipping and federated anonymization.
- **Secure Communication and IoT Systems:** Tools such as X-BELLO and HIPPALUS illustrate 8BELLS's capability to develop and secure intelligent systems in constrained and adversarial environments, further supporting use cases that require privacy-preserving AI.

In SAFE-6G, 8BELLS integrates these comprehensive competencies to develop a differential privacy module for secure and trustworthy MLOps, safeguarding user data throughout training and inference. This approach aligns with the trustworthiness objectives of 6G and proactively addresses regulatory frameworks such as the EU AI Act and GDPR compliance requirements for AI-driven network services.

3.3.12.2 FOREGROUND CONTRIBUTIONS

8BELLS contributes to SAFE-6G through the development of modular, privacy-preserving component, enabling secure deployment of machine learning services across a distributed 6G infrastructure. This includes the integration of differential privacy into MLOps workflow to ensure data confidentiality during both training and inference.

Asset #1

- **Asset Name:** Differential Privacy Module for MLOps
- **Asset Type:** Software Component / Toolkit

- **Description:**
A software module enabling privacy-preserving AI operations by incorporating techniques such as noise injection, n. Designed to operate at the edge or within federated learning systems, it safeguards sensitive data while maintaining model accuracy.
- **Availability:**
Packaged for integration into standard MLOps frameworks post-project, with licensing options for telecom operators, AI developers and cloud providers.
- **Protection:**
Protected under copyright and governed by the SAFE-6G Consortium Agreement. Use beyond the project requires formal licensing and authorization.

Asset #2

- **Asset Name:** 6G Cost-Benefit and Business Model Toolkit
- **Asset Type:** Strategic Consulting Toolkit / Analysis Framework
- **Description:**
A decision-support tool for assessing the economic viability of 6G deployment, tailored for specific use cases through CAPEX/OPEX modelling. It integrates technical metrics with market forecasts and supports ROI analysis for telecom vendors and policymakers.
- **Availability:**
Offered as a commercial consultancy package and internal analysis resource; may be partially disseminated through SAFE-6G outputs.
- **Protection:**
Proprietary toolkit; methodologies and data models protected through internal documentation and licensing agreements.

Asset #3

- **Asset Name:** SAFE-6G Market Intelligence Reports and Seminar Series
- **Asset Type:** Training / Dissemination Material
- **Description:**
Expert-curated insights into 6G business models, legal frameworks and deployment strategies. Delivered as whitepapers, webinars and strategic workshops to promote adoption and technology transfer.
- **Availability:**
Disseminated to consortium members and stakeholders via public and targeted engagement.
- **Protection:**
8BELLS retains rights to all publications; redistribution controlled under NDA or licensing terms.

Strategic Goals

As both a technological innovator and exploitation coordinator, 8BELLS aims to:

- Advance its portfolio in **privacy-preserving AI and MLOps**, extending its capabilities into **6G infrastructure**.
- Lead the development of **exploitation strategies** and **technology transfer frameworks** across the consortium.
- Produce detailed **cost-benefit analyses** and **market opportunity assessments** to support business model development for SAFE-6G use cases.

- Validate the application of **differential privacy in real-world telecom scenarios**, strengthening the position of 8BELLS as a trusted provider of secure telecom solutions.

3.3.12.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

8BELLS views SAFE-6G as a strategic opportunity to extend its influence in both the technology and market dimensions of 6G. The key exploitation themes include:

- **Market Intelligence Services:** Through the production of market reports and seminars addressing 6G business models and deployment strategies.
- **Cost-Benefit Modelling:** Focusing on CAPEX and OPEX analyses for user-centric 6G scenarios.
- **Technology Transfer Consultancy:** Facilitating the adoption of differential privacy in operational telecom systems, particularly where **AI-based services** operate over sensitive user data.

8BELLS also sees a strong opportunity to commercialize its findings by offering privacy-by-design toolkits for MLOps environments in 6G verticals such as healthcare, smart cities and defence communications.

Marketable Products and Services

Outcomes from SAFE-6G will evolve into marketable offerings such as:

- **Differential Privacy Plugins** for MLOps pipelines, adaptable to commercial AI frameworks.
- **Secure Data Analytics Modules** tailored for edge/cloud-native 6G infrastructures.
- **Professional Services** in technology transfer, standards alignment and IPR strategy formulation.

These offerings fit seamlessly into 8BELLS's existing business model, reinforcing its position as a specialist in secure digital transformation and telecom R&D.

SAFE-6G supports 8BELLS in three strategic dimensions:

1. **Technology Leadership:** highlighting 8BELLS' role in privacy-preserving MLOps and federated AI.
2. **Market Readiness:** Leveraging private 5G testbeds and real-world deployments to validate and refine product-market fit.
3. **Thought Leadership:** Publishing impactful analyses and driving community discourse on 6G monetization and ethical deployment.

8BELLS's market position is reinforced by its collaboration with **major industry leaders**, including **Airbus, Ericsson, Nokia, Thales, Leonardo** and its **engagement in 10 EDF projects**, where its solutions are trusted in high-security environments.

Total Addressable Market (TAM)

8BELLS targets the growing AI in telecom market, particularly focused on Europe. The specific TAM for privacy-preserving AI in telecom remains emerging but is projected to rapidly expand due to tightening data privacy regulations (e.g., GDPR, ePrivacy).

Current Market Position

8BELLS is a recognized SME leader in telecom-focused security R&D in Europe. The company has been consistently involved in EU-funded research, contributing high-value IP to multiple flagship projects. Its reputation in security, privacy and exploitation coordination makes it a key partner for future commercial partnerships in the 6G space.

Impact on Business Performance

8BELLS expects SAFE-6G to deliver measurable impact:

- Increased consultancy and licensing revenues through differential privacy services.
- Strengthened brand recognition as a privacy and exploitation leader.
- Expansion of its IP portfolio in the domain of privacy-preserving machine learning.

Roadmap Alignment

8BELLS's roadmap focuses on growing its role in the 6G research-to-market pipeline by:

- Consolidating its position as Exploitation and Innovation Manager in large-scale consortia.
- Developing modular privacy solutions that are technology-agnostic and standards-compliant.
- Leveraging findings to influence policy, investment and standardization discussions at the European level.

Competitive Landscape and Risks

Key competitors include major telecom vendors (e.g., Ericsson, Nokia) and privacy-focused AI startups. However, 8BELLS differentiates itself through:

- Agility as an SME and ability to lead exploitation and innovation tasks in large consortia.
- Specialized expertise in telecom-specific security and privacy protocols.

Risks include:

- Evolving regulatory landscapes around AI and data protection.
- Fast-moving AI startups that may challenge incumbent IP in differential privacy.

3.3.12.4 EXPLOITATION PLAN SUMMARY

8BELLS will capitalize on its role in SAFE-6G by delivering both technical innovation in privacy-preserving MLOps and strategic value through exploitation management. The integration of differential privacy into the AI lifecycle of 6G networks provides a unique selling point that 8BELLS can commercialize through toolkits, licensing, consultancy and training services.

Simultaneously, 8BELLS will extend its business development activities via dissemination of market intelligence, CAPEX/OPEX modeling and seminar-based engagement with stakeholders. These actions support a dual path of technology exploitation and thought leadership, ensuring long-term competitiveness in the privacy-enabled 6G economy.

<i>Innovation</i>	<i>To be Exploited By</i>	<i>Type of Exploitation (after project ends)</i>	<i>Competition, Strengths, Weaknesses, Risks (C, S, W, R)</i>	<i>Conflicting IP</i>	<i>Time-to-Market (after project end)</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
Differential Privacy for MLOps	8BELLS	Software module / Licensing / Consultancy	C: AI privacy startups, telecom vendors. S: Unique integration in 6G MLOps, strong privacy expertise. W: Limited deployment scale. R: Fast-paced AI evolution.	None identified	12–18 months	AI in telecom, edge computing, Industry 4.0	increase in service and licensing revenue
CAPEX/OPEX Business Models for 6G	8BELLS	Market analysis reports / Strategic consulting	C: Consulting firms. S: Deep technical alignment with 6G use cases. W: Niche audience. R: Market adoption pace of 6G.	None	6–12 months	Telecom vendors, network planners, EU policy makers	Expansion of market footprint and consulting revenue
6G-Focused Market Reports & Seminars	8BELLS	Training, Workshops, Reports	C: Industry analysts. S: Strong consortium insights, innovation manager role. W: Dependence on market interest. R: Low engagement from industry.	None	6 months	Telecom industry stakeholders, SMEs, verticals	New partnerships and visibility across EU market
Technology Transfer & IPR Management	8BELLS	Consultancy / IPR support services	C: Legal/IP consultants. S: In-project knowledge, direct access to partners. W: Non-scalable service. R: Regulatory complexity.	None	6–12 months	EU R&D consortia, SMEs, 6G tech providers	Long-term positioning as trusted exploitation lead

Table 16: Summary of Exploitable Results (8BELLS)

3.3.13 CUMUCORE OY EXPLOITATION PLAN

CUMUCORE is a key partner in the SAFE-6G project, contributing its expertise in 5G/6G core technology to advance private industrial network capabilities. By leveraging its proven background technologies and integrating new innovations from the project, CUMUCORE aims to enhance the scalability, security and flexibility of private industrial communication networks. Below is a comprehensive outline of its contributions, forming the basis of its exploitation strategy.

3.3.13.1 BACKGROUND CONTRIBUTIONS

CUMUCORE provides a suite of advanced, commercially available technologies as part of its background contributions:

- **CUMUCORE 5G/6G Core:** A comprehensive and scalable packet core solution designed for private industrial networks.
- **Network Slice Manager:** Enables optimized resource allocation and efficient network slicing for diverse use cases.

- **5GLAN and TSN Functionalities:** Supports seamless connectivity and ensures precise time-sensitive networking capabilities for industrial applications.

These technologies are made available to SAFE-6G project partners in binary format, accompanied by REST interface documentation for integration purposes. The key conditions for their use include:

- **Ownership:** CUMUCORE retains full intellectual property rights over all provided technologies.
- **Usage Restrictions:** The technologies are strictly for research within the SAFE-6G project. Any commercial use requires a separate licensing agreement.
- **Exploitation Conditions:** Any exploitation outside the project must be accompanied by a formal exploitation agreement, including financial terms and royalty agreements.

Through these contributions, CUMUCORE ensures that its proprietary technologies support the SAFE-6G consortium while maintaining their commercial integrity.

3.3.13.2 FOREGROUND CONTRIBUTIONS

As part of the SAFE-6G project, CUMUCORE is advancing its product portfolio through the development of an enhanced 5G Core asset:

Asset #1

- **Asset name:** 5G Core
- **Asset Type:** Platform Component
- **Description:** A next-generation packet core software platform designed for private industrial networks, integrating advanced security, reliability and usability features.
- **Availability:** Provided to consortium partners in binary format during the project; post-project access requires formal agreements.
- **Protection:** Proprietary intellectual property rights safeguard the technology, ensuring commercialization through licensing agreements.
- **Exploitation Limitations:** While available for research within the project, the asset is not authorized for commercial use without explicit licensing arrangements.

With this enhanced 5G Core, CUMUCORE addresses critical gaps in private industrial networks, focusing on seamless deployment, security and usability enhancements.

Strategic Goals

Through the integration of its background technologies and the development of new foreground assets, CUMUCORE aims to:

- Strengthen the scalability and security of its 5G core for industrial deployments.
- Validate its technology through real-world testing with SAFE-6G partners.
- Establish a commercialization pathway aligned with emerging 6G standards.

3.3.13.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

The core of CUMUCORE's SAFE-6G exploitation strategy lies in integrating additional network functions to enhance the security, reliability and usability of its existing 5G core product. The

opportunity comes from packaging new components, such as security and reliability functions and chatbot-based usability enhancements.

Business opportunities arise from:

- **Improved Security Features:** Enhancing the resilience of private mobile networks through new security modules.
- **Advanced Reliability Functions:** Implementing high-availability solutions based on 3GPP-defined Group SET ID, ensuring fault tolerance.
- **Enhanced Usability with AI-driven Support:** Leveraging chatbot functionality to improve the user experience.

By integrating SAFE-6G modules and collecting usability feedback from partners, CUMUCORE can refine its product offerings and increase its market potential.

Marketable Products and Services

The SAFE-6G functions developed by CUMUCORE will be incorporated into its existing portfolio, offering:

- **Next-Generation Private Mobile Networks:** With enhanced security and reliability.
- **Customized Network Slicing and TSN Services:** Targeted solutions for industrial automation and enterprise networks.
- **AI-driven Support Services:** Improved network management through chatbot integration.

These additions will strengthen CUMUCORE's competitive position and open up new revenue streams.

CUMUCORE's commercialization strategy includes:

- Strengthen the scalability and security of its 5G core to meet industrial demands.
- Validate its technology in real-world scenarios through collaboration with consortium partners.
- Establish a clear commercialization pathway for post-project market entry, aligning its solutions with emerging 6G standards.

Intermediate steps involve testing, partner feedback collection and iterative improvements, ensuring the readiness of SAFE-6G functions for market adoption.

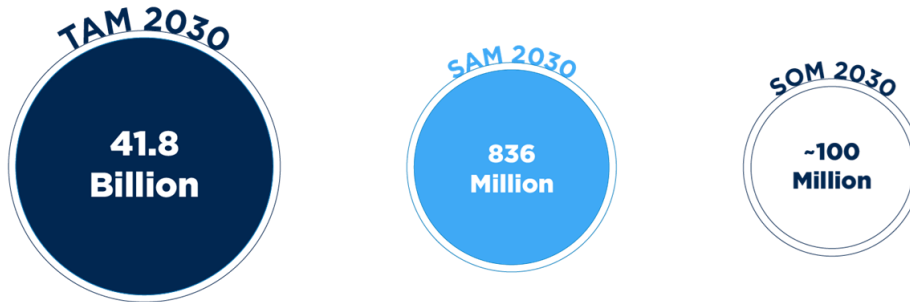
Total Addressable Market (TAM)

Market studies indicate a potential deployment of **4 million private networks**, aligning with CUMUCORE's focus on private industrial communications.



Market Size

Global Private 5G Network Market CAGR of 49.7% from 2021 to 2030



Source: www.grandviewresearch.com

4

Figure 6: Global Private 5G Network Market Forecast

Current Market Position

CUMUCORE is recognized as a leading provider of private mobile networks, with a growing reputation among industrial clients. However, specific market share figures remain undisclosed.

Impact on Business Performance

CUMUCORE anticipates a **30% increase in revenue** following the integration of SAFE-6G security and reliability functions. The enhanced product offerings will solidify its position in the market and expand its customer base.

Roadmap and Standards Alignment

CUMUCORE provides a single product that consists of mobile packet core. SAFE-6G functions would be an add-on which customers can select to add on top of the basic product.

Competitor Analysis

Major competitors in the space include:

- **Large Vendors:** Nokia, Ericsson, HPE.
- **Medium-sized Competitors:** Druid, Celona.

Competitive Advantages through SAFE-6G

CUMUCORE's participation in SAFE-6G reinforces its differentiation by:

- Offering modular security and reliability features for private 5G/6G networks.

- Leveraging AI-based usability improvements for better customer experience.

3.3.13.4 EXPLOITATION PLAN SUMMARY

The exploitation plan of CUMUCORE in SAFE-6G consists of design of additional network functions that can be integrated into 5G core to enhance the security, reliability and usability. The exploitation opportunity comes from the packaging of new components such as Security, Reliability functions and Chatbot that will improve security and usability of current 5G core product. CUMUCORE will validate in SAFE-6G the new network functions which could be integrated into the current packet core. The added value of the SAFE-6G network functions consists of improving security that should increase the value of the product. Moreover, usability improvements through the integration of chatbot would provide better user experience when utilizing CUMUCORE product which contributes to the monetization.

The role of CUMUCORE in cooperation with the partners to ensure the SAFE-6G functions are 3GPP compliant will facilitate interoperability and integration with standard compliant product, which facilitates the commercialization. Moreover, the usage of CUMUCORE together with SAFE-6G network functions within the consortium provides the required validation to ensure the integration of the whole system and will help improving final product based on the feedback from the partners deploying CUMUCORE system on their laboratories.

<i>Innovation To be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition Strengths Weaknesses Risks (R)</i>	<i>(C), (S), (W),</i>	<i>Conflict ing IP</i>	<i>Time-to-Market</i>	<i>Targeted Market</i>	<i>Expected ROI</i>
SDP (Integrated in Safety Function)	CUMUCORE	Product	C: Nokia, Ericsson, Celona S: Standards-compliant, modular security W: Market visibility R: Regulatory barriers	None	2 years	Private mobile networks	30% revenue increase

Table 17: Summary of Exploitable Results (CUMUCORE)

By validating its SAFE-6G contributions and ensuring standard compliance, CUMUCORE is well-positioned to expand its market share in private industrial n

3.3.14 IMMERSION EXPLOITATION PLAN

Immersion (IMM), a key partner in the SAFE-6G project, contributes cutting-edge expertise in XR, virtual collaboration and human-machine interaction. By combining its established background knowledge with new innovations developed during the project, IMM aims to address challenges in interactive visualization, training and collaborative decision-making within next-generation network environments. Below is a detailed description of its contributions, forming the basis of its exploitation strategy.

3.3.14.1 BACKGROUND CONTRIBUTIONS

IMM's contributions are part of the **Shariing ecosystem**, utilizing many of its solution components and intellectual properties. IMM provides extensive knowledge and tools as part of its background contribution, focusing on:

- **Design and Production Expertise:** Hardware and software solutions for XR environments, including augmented, virtual and mixed reality interactions.
- **Collaborative Tools and Techniques:** Advanced methods for synchronous remote collaboration and interactive decision-making.
- **Interaction Data Processing:** Real-time data analysis and AI-driven decision support.
- **Embedded 3D Rendering Solutions:** High-performance rendering for immersive and interactive applications.
- **Human-Machine Interaction Engineering:** Implementation of haptic, tangible interfaces and adaptive user experiences.
- **Mixed Reality-Assisted Manufacturing:** Integration of XR tools into industrial workflows, building upon insights from previous projects like EVOLVED-5G.

Implementation & Exploitation Limitations:

- IMM's background knowledge is exclusively for SAFE-6G project use, both in duration and scope. Any use beyond the project requires written approval.
- IMM's background technology cannot be commercially exploited outside the project.

Through these contributions, IMM provides foundational expertise to advance **XR-driven innovation within the SAFE-6G framework**.

3.3.14.2 FOREGROUND CONTRIBUTIONS

IMM is developing two key XR applications within SAFE-6G:

Asset #1

- **Asset Name:** Digital Factory Metaverse Application
- **Asset Type:** Application
- **Description:**
 - A Unity-based digital twin for factory environments.
 - XR-enabled interaction for end-users to resolve production issues and optimize configurations.
 - Integration of a virtual chatbot to interact with SAFE-6G components.
- **Availability:**
 - Deployable on XR devices and workstations for project validation.
 - APIs and endpoints may be exposed for remote interaction.
- **Protection:**
 - IMM retains IP rights, including copyright, trademarks and patents.
 - Confidentiality agreements (NDAs), access control and digital watermarking will be used to protect assets.
- **Exploitation Limitations:**
 - IMM retains full IP rights; any dissemination or reuse requires explicit consent.

- Distribution of application components requires prior written approval from IMM.
- **Status:** 20% complete.

Asset #2

- **Asset name:** Formation Metaverse Application
- **Asset Type:** Application
- **Description:**
 - A Unity application using XR+AI to facilitate industrial training and certification for production line workers.
 - Enables users to visualize machine procedures in XR and simulate training steps.
 - Includes a chatbot interface for interacting with SAFE-6G components.
- **Availability:**
 - Deployed on XR devices and workstations during project validation tests. APIs and endpoints may be exposed for remote interactions.
- **Protection:**
 - Intellectual property protection mechanisms such as Soleau letters or patents will be applied as necessary during project evolution. The source code, software components and unique designs are protected under copyright law. Even in the absence of Soleau letters or patents, all contributions are protected under the Consortium Agreement governing the SAFE-6G project, ensuring that ownership and rights are clearly defined and enforced. Additional measures include:
 1. Confidentiality Agreements (NDAs): If required external collaborators, partners and stakeholders will need to sign non-disclosure agreements with IMM to maintain confidentiality regarding the application's technical details and innovations.
 2. Access Control: Access to source code, software assets and deployment configurations is strictly restricted to authorized personnel.
 3. Digital Watermarking: Digital assets, including 3D models and other graphical elements, will be protected using watermarking techniques to trace unauthorized use or reproduction.
 4. Registration of Design and Branding: The application's interface, visual elements and branding will be registered as industrial designs to protect the distinct appearance of the platform.
- **Exploitation Limitations:**
 - Dissemination and exploitation require IMM's explicit written consent. IMM retains IP rights, including trademarks, patents and copyrights.
 1. **Usage Restrictions:** Use of IMM's knowledge is restricted exclusively to the SAFE-6G project, both in terms of duration and scope. Any use beyond the SAFE-6G program, or for any other implementation or project, is strictly prohibited without prior written approval.
 2. **No Reuse Without Authorization:** No part of the software, including APIs, XR functionalities, or chatbot components, may be reused, modified, or integrated into other projects without IMM's explicit

consent. This restriction applies regardless of whether the reuse occurs within or outside the SAFE-6G project scope.

3. **Distribution Control:** Distribution of the application, in part or in whole, must be explicitly authorized by IMM. Redistribution or modification of any components, including the virtual chatbot interface, requires prior written approval from IMM
 - **Status:** 20% complete.

Strategic Goals

IMM's contributions to SAFE-6G align with its core strategy of enhancing **Shariing offerings** with **6G-enabled XR applications**. Key objectives include:

- Enhance XR-driven innovation in industrial environments through Digital Factory and Formation Metaverse applications.
- Validate XR solutions in collaborative and training use cases, leveraging the SAFE-6G platform.
- Establish commercialization pathways aligned with IMM's IP and product strategy, while maintaining control over its assets.
- Implement XR application solutions leveraging high-fidelity content streaming techniques on Android and iOS devices over high-performance networks. In this context, 6G could be a particularly promising candidate for such mobile applications.

3.3.14.3 EXPLOITATION STRATEGY & MARKET OPPORTUNITIES

One standout exploitation opportunity for IMM in the SAFE-6G project is the use of DT streaming and professional formation in mobility experiences. Major French industrial players are already in discussions with IMM to find a secure and intelligent solution to replace their existing Wi-Fi networks in their factories. While private 5G networks have been deployed at numerous client sites, their practical use is still limited. IMM aims to leverage the advancements from SAFE-6G to demonstrate a compelling use case that aligns closely with these industrial needs, providing the confidence and value proposition necessary to encourage these clients to invest in next-generation network solutions. IMM's ambition is to showcase how DT applications, streamed seamlessly over high-performance 6G infrastructure, can transform industrial operations and mobility, driving both efficiency and innovation.

Marketable Products and Services

For IMM, SAFE-6G is the opportunity to explore the capabilities and services proposed by 6G networks. This way, IMM will be able to adapt its existing XR and collaboration solutions to Trustworthiness-oriented 6G network infrastructures. The related research and implementation efforts will allow the company to stay at the edge of innovation in terms of collaborative solutions and prepare the next generation of products and immersive spaces. Thanks to these efforts, IMM will continue to address the growing market of collaborative XR+AI solutions, which is expanding quickly since the recent progress of immersive technologies. IMM will leverage its core technology called Shariing, to which the company will add dedicated services addressing these network-related challenges.

The first products resulting from the project will be the 6G-enabled metaverse use-cases applications. Both the Factory Digital Twin and the Formation metaverse applications will integrate a virtual chatbot service to let users define their priorities in terms of Security, Safety, Resilience, Reliability and Privacy. Both applications will be used as demonstrators at the end of the project.

Besides, another envisioned product is an all-included metaverse kit based on CloudXR and compliant with the Shariing solution. This kit, contained within a transport suitcase, will allow users to easily prepare, run and stream a Unity application from an integrated workstation to an XR headset. In addition to being a turnkey solution for industrial and academic clients, this product will also be a valuable asset for IMM to facilitate demos performed at professional exhibitions. Nvidia is currently in discussions with IMM to become a major player in deploying cloud XR technology, further enhancing the potential of this product by allowing users to quickly discover the capabilities related to such streaming technology.

These products register themselves in IMM's portfolio as the direct evolution of their predecessor. After the exploration of the potential of 5G within the EVOLVED-5G EU project, the company further explores the capability of innovative network infrastructure to continue to innovate and propose the best collaborative setups to its clients and partners.

Path to Market

IMM has the required expertise and assets to develop both metaverse applications. The SAFE-6G project will enable IMM to achieve the integration of 6G features related to the chatbot and trustworthiness aspects.

Moreover, the company has significant experience in the design and integration of portable solutions, such as XR kits and immersive environments, which will facilitate the creation of an initial prototype kit to be tested during the SAFE-6G project. This prototype will then undergo further refinement and standardization before officially being integrated into IMM's portfolio of solutions.

The envisioned path to market includes the following steps:

- **Conduct Market Analysis Research:** This includes validation with key industrial stakeholders to ensure alignment with market needs and expectations.
- **Assess the Expected Market Impact:** Evaluating potential impact by conducting feasibility studies and working closely with industry partners to validate use cases.
- **Development of Initial Prototype:** Design of the first prototype, leveraging our expertise in integrating XR components within portable kits, to be deployed and tested during SAFE-6G.
- **Testing and Iterative Refinement:** Gather feedback from SAFE-6G partners and other selected users during the validation phase. The prototype will be iteratively refined based on real-world testing and partner input.
- **Standardization and Market-Ready Product:** Refine and standardize the prototype to obtain a marketable product, ensuring scalability and reliability.
- **Launch of the CloudXR Kit on IMM's Marketplace:** The final version of the CloudXR kit will be launched on IMM's marketplace. This will be complemented by strategic partnerships, including discussions with Nvidia, to support the deployment of cloud XR technologies. These

partnerships will help to maximize the potential of the solution by enabling users to quickly discover the capabilities of DT streaming over next-generation network infrastructure.

Near-Term Applications

The CloudXR kit is the most suitable envisioned product for near-term application, as it could potentially even be used without 6G (for instance, with an adapted Wi-Fi 6 router). While the two metaverse use-case applications will be functional at the end of the project, part of their added value will only come with the mid/long term development of Trustworthiness-based 6G networks.

Total Addressable Market (TAM)

As a leading SME in XR and collaborative solutions, IMM targets the growing market of immersive technologies in Europe, working with both industrial and academic partners. The total addressable market (TAM) for immersive technologies in Europe is projected to reach approximately €55 billion by 2025, with a compound annual growth rate (CAGR) of 48%, driven by the increasing adoption of XR across various sectors, including Industry 4.0, education and training.

- **UC1: Industry 4.0 Focus:** UC1 primarily targets Industry 4.0 companies across key sectors such as automotive, aerospace and manufacturing. The European Industry 4.0 market, which includes immersive solutions for process optimization and workforce training, represents an estimated €12 billion opportunity by 2025, with Germany and France being primary regions due to their robust industrial base and government incentives promoting technological innovation.
- **UC2: Education and Hybrid Training:** UC2 aims to address a wide spectrum of educational and hybrid training environments. The immersive education and professional training market in Europe is expected to reach €8 billion by 2026. Key locations include France, the UK and Spain, where educational institutions and professional training programs are increasingly adopting XR solutions to enhance learning outcomes.

Current Market Position

Immersion is a key player in the XR and collaborative solutions market, both in France and at the European level. With 30 years of experience, the company has built a solid reputation and is well-positioned as a trusted partner for some of the largest industry players, such as Renault, Airbus, Dassault Systèmes and the CEA.

Immersion specializes in providing cutting-edge immersive and interactive systems, including large-scale image walls, collaborative tables and head-mounted displays, all integrated into highly functional and user-friendly environments. The company's expertise also extends to the development and distribution of its proprietary Shariing solution, which is widely adopted for collaborative work in industrial, research and academic contexts.

On the French market, Immersion is recognized as a leader, holding a significant share in the deployment of immersive solutions for Industry 4.0 and collaborative workspaces. The company has also been involved in creating and implementing immersive showrooms and collaborative

environments for industries ranging from automotive to aerospace and luxury goods, thus ensuring a strong foothold across diverse economic sectors.

At the European level, Immersion has established itself as a significant player through participation in major projects and partnerships across different countries. The company is engaged in several European R&D projects focusing on XR, which helps maintain its position at the forefront of innovation while expanding its reach and network across the continent.

In terms of distribution, Immersion leverages a well-established network of industry and academic partners, enabling it to place its solutions directly in environments where innovation is key. The current annual revenue is approximately €7 million, reflecting the growing demand for high-quality, immersive solutions across its client base.

Immersion's competitive advantage is also driven by its commitment to end-to-end customer support—from the conception of customized immersive environments to the development of tailored software solutions and the ongoing technical assistance provided to its customers. This comprehensive approach has allowed Immersion to establish long-term relationships and high customer loyalty with industry giants such as Renault, Airbus, SNCF and L'Oréal.

Additionally, Immersion has benefited from partnerships with major technology providers, such as Nvidia, to support cloud XR initiatives, thereby adding value to its product offering. This positions the company as a strong partner not only for immersive hardware and software but also as a pioneer in the cloud-based streaming of XR content, targeting future market needs with next-generation 6G connectivity.

In summary, Immersion's current market position is characterized by its strong industrial partnerships, expansive experience, broad product offering and leadership in the integration of immersive technologies for collaborative and industrial use cases. This market positioning, backed by its innovative solutions and strategic partnerships, ensures Immersion's relevance and growth within the rapidly expanding XR sector.

Impact on Business Performance

IMM's current revenue from the distribution of XR solutions is estimated at €2 million, of which €1 million is attributed to headset sales. IMM aims to leverage the CloudXR capability to increase the value of its offerings. If IMM successfully sells the CloudXR option to 10% of headset buyers and if this option multiplies the value of the initial purchase by four:

- Number of Customers Adopting CloudXR: 10% of the headset buyers.
- Revenue Increase per Customer: The CloudXR option quadruples the initial value of the purchase.

Thus, the expected increase in revenue can be calculated as follows:

- Additional Revenue:

- 10% of €1 million = €100,000 (value of headsets sold to customers opting for CloudXR).
- Quadrupling this value results in an additional €300,000.

Therefore, IMM could expect an increase in revenue of approximately €300,000, bringing the total revenue from XR distribution to €2.3 million. This represents a significant opportunity for growth and a strong potential to enhance the overall value proposition of IMM's XR product portfolio.

By targeting both Industry 4.0 and educational/training markets and capitalizing on the CloudXR offering, IMM is well-positioned to capture value across diverse sectors, ensuring strong alignment with current market needs while significantly increasing revenue potential.

Roadmap and Standards Alignment

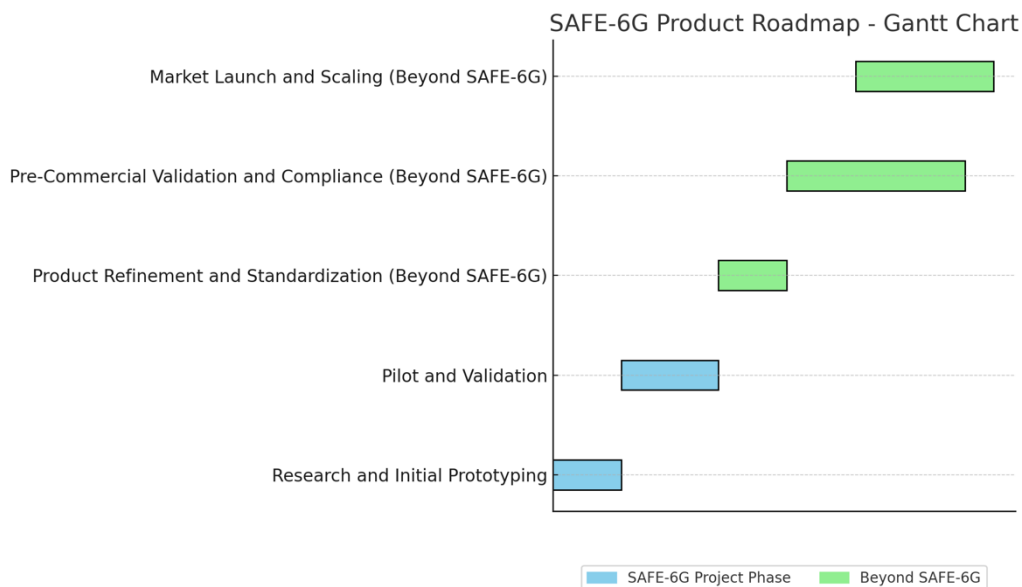


Figure 7: SAFE-6G Product RoadMap - Gantt Chart

1. Research and Initial Prototyping
 - a. Conduct market research and analyze requirements in collaboration with industry stakeholders to define features aligned with Industry 4.0 and education needs.
 - b. Develop an initial prototype of the CloudXR solution, integrating 6G capabilities such as secure chatbots and trustworthiness features.
 - c. Perform internal testing to ensure compatibility with current network infrastructure and future 6G developments.
2. Pilot and Validation
 - a. Deploy prototypes in pilot environments with selected industrial and academic partners.
 - b. Gather feedback from users to validate the technology’s effectiveness, particularly focusing on streaming quality, data security and end-user interaction.
 - c. Collaborate closely with partners like Nvidia to refine and optimize the CloudXR integration.

(From this point forward, activities are beyond the scope of the SAFE-6G program)

3. Product Refinement and Standardization
 - a. Iterate on the prototype based on user feedback, refining both the hardware kit and the software integration.
 - b. Standardize production processes and finalize the product design, ensuring scalability and reliability for broader market adoption.
4. Pre-Commercial Validation and Compliance
 - a. Ensure regulatory compliance, particularly for data security and interoperability standards.
 - b. Validate the production and distribution processes to prepare for a successful market launch.
5. Market Launch and Scaling
 - a. Launch the finalized CloudXR kit through IMM's marketplace and leverage existing distribution channels.
 - b. Increase visibility through demonstrations at professional exhibitions and develop strategic partnerships to drive adoption.
 - c. Expand the market reach by targeting additional sectors such as healthcare and public services.

Our targeted fields and tasks in the SAFE-6G project align closely with our strategic roadmap in several key areas:

XR Innovation:

- Digital Factory Metaverse Application: This aligns with our goal to enhance industrial environments through advanced XR solutions. By creating a DT for factories, we aim to improve production line efficiency and problem-solving capabilities to attract new Industry 4.0 customers.
- Formation Metaverse Application: This supports our objective to revolutionize industrial training and certification processes using XR and AI technologies.

Collaborative Decision-Making:

- Our focus on developing tools for synchronous local and remote collaboration directly supports our roadmap's emphasis on improving decision-making in collaborative environments. This includes real-time data analysis and machine learning to enhance user interactions and outcomes.

Current State of the Art and Competitor Analysis

The potential competition could arise if a provider of XR software solutions teamed up with another provider specializing in XR streaming to develop similar and competing products. Given this possibility, it is essential to examine the state of the art in XR streaming solutions to better understand the potential competition.

NVIDIA CloudXR is currently one of the most advanced solutions for streaming XR content, encompassing both virtual reality (VR) and augmented reality (AR). This technology allows immersive experiences to be streamed from a remote server to an XR headset, smartphone, or tablet over high-performance networks such as 5G and Wi-Fi 6. CloudXR leverages GPU power to deliver high-quality graphics without requiring the user to invest in expensive or bulky hardware. It is compatible with major VR platforms such as Vive, Oculus and Windows Mixed Reality and supports cloud infrastructures like AWS and Microsoft Azure, making it particularly appealing for industrial and commercial applications.

HTC also offers an XR streaming solution via its Viveport Streaming platform, which enables games and VR applications to be streamed from a high-performance PC to standalone VR headsets such as the Vive Focus. Using Wi-Fi technology, Viveport allows for immersive experiences without the user being physically tethered to the PC, providing greater freedom of movement while ensuring the necessary computing power for complex graphics.

Meta, formerly known as Facebook, launched Air Link, a feature that allows VR content to be streamed from a PC directly to Oculus or Meta Quest headsets. Air Link works over a high-performance local Wi-Fi network, enabling users to play PC VR games wirelessly while maintaining near-wired quality. Although primarily aimed at consumers, this solution points the way towards making high-quality VR content accessible without the limitations of onboard hardware.

AMD offers Radeon ReLive VR, a solution that allows users to enjoy VR on standalone or mobile headsets without cables. Similar to NVIDIA CloudXR, Radeon ReLive VR leverages the computing power of AMD graphics cards to stream high-quality immersive experiences. While it is primarily focused on gaming, this solution is also relevant for professional applications due to the quality of its streaming and low latency.

Another notable solution is Virtual Desktop, which allows PC content to be streamed to VR headsets such as the Meta Quest 2. Virtual Desktop initially started as a way to use office applications in VR but quickly expanded to include VR games and other immersive applications. Unlike solutions like CloudXR, Virtual Desktop does not rely on dedicated cloud infrastructure but rather on the user's local network, offering a lower-cost alternative to cloud-based solutions.

Public cloud solutions, such as Amazon Web Services (AWS), Google Cloud and Microsoft Azure, also play a significant role in XR streaming development. These platforms enable XR experiences to be deployed at scale, with graphical rendering executed directly in the cloud. This allows immersive video streams to be delivered to end-users, who can interact with these environments in real time. This type of deployment is extremely scalable, particularly suitable for industrial contexts where reducing the costs associated with VR equipment is crucial.

In summary, the state of the art in XR streaming solutions demonstrates a strong dynamic of innovation and diversification in market offerings. Solutions such as NVIDIA CloudXR, HTC Viveport Streaming, Meta Air Link, AMD Radeon ReLive VR, Virtual Desktop and public cloud platforms show different approaches to making immersive experiences more accessible while minimizing hardware limitations. These technologies, although promising, present challenges such as reliance on the quality

of the network connection, costly investments to ensure low latency and sufficient bandwidth and issues related to data security and privacy. This indicates that the XR streaming market is not only growing but also constantly evolving, providing significant opportunities for players capable of innovating and adapting to changing user needs.

Opportunities and Threats

Opportunities: high and quickly expanding demand for XR+AI collaborative solutions and spaces. Growing attention dedicated to network security and trustworthiness. Partnership with telecom providers and tech companies can enhance market reach and innovation. Extensive experience and expertise of IMM about XR and collaboration.

Threats: Alone, IMM has limited technical knowledge about 5G and 6G networks. Besides, XR is a quickly advancing field, especially now combined to IA solutions. Competitors include major tech companies with already established userbases, hardware and ecosystems of solutions.

3.3.14.4 EXPLOITATION PLAN SUMMARY

IMM's exploitation plan for SAFE-6G products is centred around leveraging its expertise in XR and immersive solutions to capitalize on the growing demand for Industry 4.0 innovations and advanced educational tools. The primary focus is to take advantage of the novel capabilities enabled by 6G to deliver enhanced DT streaming, immersive collaboration and mobility-focused XR experiences. The plan involves both direct commercialization and strategic partnerships to reach industrial and educational clients effectively.

Market Opportunities: The core product includes an all-in-one CloudXR solution integrated with IMM's proprietary Shariing platform. This product is targeted at high-value sectors such as automotive manufacturing, aerospace and advanced research institutions. The initial target is European markets with high industrial concentration, where the adoption of immersive technologies is growing rapidly.

Phased Commercial Rollout:

1. **Prototype Validation:** The SAFE-6G project will validate the initial prototypes with partners in both industry and academia. Feedback from these trials will guide further product refinement.
2. **Market Entry:** The refined product, a portable XR kit compatible with CloudXR, will enter IMM's portfolio for general availability. It will be distributed through IMM's established channels, leveraging existing partnerships with prominent industrial players such as Renault, Airbus and the CEA.
3. **Strategic Partnerships and Expansion:** IMM is in ongoing discussions with Nvidia to become a significant player in the deployment of CloudXR technology. This partnership is expected to strengthen the product's appeal, allowing for rapid adoption across various industries. Further expansion is planned into other European markets with growing interest in XR-driven digital transformation.

Revenue Model: The revenue model will be driven by a combination of direct hardware sales (e.g., XR kits) and service-based offerings. IMM will capitalize on the ability to bundle CloudXR capabilities as an add-on, significantly increasing the average sales price through subscription models and long-term service agreements.

Long-Term Vision: The long-term vision includes scaling this solution to support fully mobile DT streaming, leveraging advanced 6G infrastructure to enhance connectivity and user experience in dynamic industrial environments. The ultimate goal is to position IMM as a leading European provider of secure and scalable XR solutions that transform industrial and educational environments through advanced immersive technologies.

Risk Mitigation: Key risks include market readiness for 6G infrastructure and the adoption pace of XR solutions. To mitigate these risks, IMM will engage closely with partners to build early success stories, secure pilots that demonstrate value and work on gradual transitions that allow industries to shift from legacy systems to advanced XR solutions smoothly.

<i>Innovation To be Exploited By</i>	<i>Type of Exploitation</i>	<i>Competition (C), Strengths (S), Weaknesses (W), Risks (R)</i>	<i>Time-to-Market</i>	<i>Target Market</i>	<i>Expected ROI</i>	
Factory Metaverse App	IMM	Demonstrator	C: GAFAMs, Nvidia, HTC. S: Secure XR solution. W: Lack of 5G/6G expertise. R: AI disruptions.	Project End	Industry 4.0	New customers, industry collaborations.
Formation Metaverse App	IMM	Demonstrator	Same as above.	Project End	Education, Workforce Training	Expansion into hybrid training markets.
CloudXR Kit	IMM	Commercialized Product	Game-changing XR streaming tech.	T+12 months	XR Collaboration	€300,000+ revenue boost.

Table 18: Summary of Exploitable Results (IMM)

By leveraging 6G infrastructure and secure XR technologies, IMM is poised to disrupt industrial XR collaboration and training markets.

3.4 EVALUATION OF KEY EXPLOITABLE RESULTS

Based on the individual exploitation plans and the identified exploitable assets as detailed in the previous subsection, within the SAFE-6G project, the consortium undertook a structured and methodical approach to prioritize and assess the innovation outcomes. Recognizing the diversity and strategic importance of these results, a comprehensive multi-criteria evaluation form was developed and applied across all key technological outputs.

This evaluation tool was designed to provide a balanced and objective analysis of each exploitable result, considering multiple dimensions—such as technological maturity, commercial potential, strategic fit and ecosystem impact. Specifically, the assessment focused on ensuring that each innovation is not only technically relevant but also positioned for successful deployment and adoption within the broader 6G landscape.

The evaluation framework served multiple complementary functions. **First**, it enabled the consortium to systematically rank and benchmark the exploitable results, highlighting those with the highest potential for commercial uptake, societal impact and technological leadership. **Second**, it provided actionable insights that informed the refinement of exploitation strategies, both at the individual partner level and at the consortium level. These insights also guided the identification of suitable pathways for technology transfer, whether through licensing, joint ventures, standardization, or direct market entry.

Additionally, the outcomes of this structured assessment contributed to an internal understanding of investment readiness for each result—enabling partners to plan for targeted funding opportunities, stakeholder engagement and external partnerships aligned with their exploitation ambitions.

Finally, this evaluative process strengthened the consortium’s ability to convert research outputs into tangible value, fostering a well-aligned trajectory from innovation to impact across the SAFE-6G project's lifecycle.

Evaluation Criteria Overview

To ensure a comprehensive assessment of each exploitable asset, the consortium employed an evaluation matrix structured around eight key dimensions. These criteria were carefully selected to capture the full spectrum of technical, economic, strategic and collaborative aspects necessary for successful innovation exploitation. Each result was independently scored and benchmarked against these dimensions, allowing for a nuanced understanding of its strengths, challenges and strategic fit.

Scoring Methodology

Each criterion was scored on a standardized scale from **1 to 5**, where **1** represents a low or limited value and **5** indicates a high or exceptional value. The evaluation was conducted independently by domain experts from within the consortium, ensuring objectivity and relevance based on the nature of each result. All scores were assigned through consensus during dedicated review sessions, supported by evidence such as technical documentation, market analysis, and validation results. These scores were then compiled into an evaluation matrix, allowing for benchmarking and comparative analysis across all exploitable assets.

To provide a consistent basis for comparison, each result’s total score was normalized to a percentage scale, with the highest possible composite score corresponding to **100%**. This normalization allowed for a clear ranking of all results based on their relative exploitation potential.

1 Market Potential Score – This criterion evaluates the commercial attractiveness of the result, focusing on the size and accessibility of the addressable market, the intensity of market demand and the presence of unmet needs. A higher score indicates stronger prospects for market adoption and revenue generation.

2 Innovation Level Score – Measures the degree of technological advancement and originality of the result compared to the current state of the art. This includes evaluating breakthrough

features, disruptive potential and intellectual property opportunities. High-scoring results typically demonstrate novel contributions that can differentiate the consortium's offering in a competitive 6G environment.

- 3 **Feasibility Score** – Assesses the technical maturity of the asset, particularly in terms of its readiness for real-world deployment. This includes factors such as TRL, existing prototypes, validation outcomes and integration complexity. Results with higher feasibility scores are those closest to market or demonstrator stage.
- 4 **Scalability Score** – Evaluates the potential of the technology to be expanded or adapted across different application domains, geographic regions, or user groups. Scalable results are seen as having wider applicability and are more likely to attract strategic interest from industry partners and investors.
- 5 **Economic Impact Score** – Projects the financial value the result could generate, considering return on investment (ROI), cost-effectiveness and potential for job creation or productivity enhancement. This score helps identify which innovations are likely to deliver the highest economic benefit to stakeholders.
- 6 **Alignment with Project Goals Score** – Gauges how effectively the result supports the overarching objectives of the SAFE-6G project, including trust, security, sustainability and digital sovereignty. This ensures that results not only have standalone value but also contribute to the collective impact and coherence of the project's mission.
- 7 **Sustainability Score** – Considers the long-term viability of the result in environmental, societal and operational terms. This includes energy efficiency, lifecycle costs, social inclusiveness and alignment with green ICT principles. High scores reflect technologies that align with European sustainability targets and ethical technology development practices.
- 8 **Synergy with Partners Score** – Captures the extent to which the result benefits from, or contributes to, collaboration among consortium members. This includes shared IP development, integration into joint solutions and potential for cross-partner commercialization or co-investment. Strong synergies often signal a higher likelihood of collective exploitation success.

Through this multi-dimensional evaluation approach, the SAFE-6G consortium ensured that all exploitable results were not only assessed fairly but also positioned strategically for maximum impact—technologically, commercially and societally.

	Exploitable Result	Owner	Market Potential	Innovation Level	Feasibility	Scalability	Economic Impact	Alignment with Project Goals	Sustainability	Synergy with Partners	Total
Key Exploitable Results	5G/6G core technology	CUMUCORE	100%	100%	100%	100%	100%	100%	91%	100%	100%
	MLOps Framework	Eviden	73%	75%	112%	96%	75%	90%	91%	100%	90%
	OPenCAPIF	Telefonica	81%	90%	102%	94%	65%	76%	85%	91%	86%
	Chatbot (Intent Classification)	NCSR D	83%	79%	104%	92%	75%	90%	74%	79%	86%
	XAI Assistant	THALES	80%	96%	85%	69%	78%	81%	78%	96%	84%
	Blockchain-Based SSI Framework	InQbit	73%	96%	92%	84%	85%	78%	78%	79%	84%
	AI intent driven chatbot app	INF	83%	58%	104%	88%	78%	90%	70%	79%	83%
	Formation metaverse app	IMM	63%	88%	96%	76%	78%	71%	100%	75%	81%
Emerging Assets	Factory DT metaverse app	IMM	69%	88%	92%	69%	60%	81%	100%	79%	80%
	Cognitive Coordinator	NCSR D	71%	77%	87%	82%	73%	83%	72%	88%	80%
	Resilience Function	Telefonica	66%	88%	77%	76%	67%	87%	82%	72%	78%
	Reliability Function	UNIWA	68%	81%	79%	78%	69%	86%	76%	70%	77%
	Smart Contracts for SSI & Security A	InQbit	75%	81%	79%	86%	69%	67%	72%	67%	75%
	SDP (Integrated in Safety Function)	eBOS	66%	79%	81%	73%	75%	71%	70%	68%	73%
	CloudXR kit	IMM	80%	79%	88%	69%	75%	46%	91%	58%	73%
	Meta-operating system	UPV	63%	83%	69%	80%	53%	62%	91%	65%	71%
	AI-Driven Trust Agents and Automat	InQbit	54%	69%	67%	55%	51%	60%	60%	53%	59%
	Privacy Function	SPACE	54%	60%	63%	55%	55%	54%	60%	56%	58%
	SSI system	Eviden	46%	63%	54%	57%	53%	46%	62%	47%	53%

Table 19: Exploitable Results Evaluation

Each score was weighted equally, leading to a **total composite score**, which offers a holistic view of the result's overall exploitation potential.

3.4.1 TOP-RANKED EXPLOITABLE RESULTS -KEY EXPLOITABLE RESULTS

Based on the outcomes of the multi-criteria evaluation, several key technological results emerged as particularly promising for strategic exploitation, investment targeting and early market entry. These results demonstrated a balanced combination of innovation, feasibility, scalability and alignment with both SAFE-6G project goals and the broader 6G innovation agenda. Below is a summary of the top-ranked assets, along with insights into their strategic relevance and potential impact.

Key Exploitable Results

- **5G/6G Core Technology – CUMUCORE (Score: 100%)**

This result led the overall ranking, representing a cornerstone innovation with full alignment to SAFE-6G objectives. Its exceptional scores across market potential, technical maturity and partner synergy underscore its readiness for industrial deployment. As scalable 6G core networks become a foundational element of future telecommunications, this asset is positioned for direct integration into next-generation infrastructure and standardization tracks.

- **MLOps Framework – Eviden (Score: 90%)**

The MLOps framework was identified as a strategic enabler of AI-driven automation and trustworthiness in telecom operations. High feasibility, coupled with deep integration across consortium partners, positions this asset as a critical component in operationalizing machine learning workflows, ensuring both efficiency and explainability in AI-based decision-making processes within 6G networks.

- **OpenCAPIF – Telefónica (Score: 86%)**

OpenCAPIF demonstrated strong potential in terms of feasibility, interoperability and scalability. As a standardized interface for secure and transparent service exposure, this asset aligns well with industry

needs for API openness and cross-vendor compatibility—key pillars of service innovation in open 6G architectures.

- Chatbot (Score: 83%)

The chatbot solution achieved a strong score due to its innovative approach to user interaction and its alignment with SAFE-6G's goals of trust and accessibility. It combines an intent-prediction model with a dynamically prompted large language model (LLM), allowing non-expert users to provide precise input for cognitive coordination. This enhances both data quality and user engagement. The result scored particularly well in innovation level, feasibility, and scalability, with notable potential for integration into consumer and industrial telecom interfaces. Its personalized, trust-aware interaction model supports broader 6G ambitions of user-centric and explainable AI systems.

- **XAI Assistant – THALES & Blockchain-Based SSI Framework – InQbit** (Scores: 84%)

These complementary assets reflect high innovation scores (including novelty ratings of 38) and exhibit solid feasibility for integration across trust, identity and explainability layers. The XAI Assistant contributes to transparent AI decision support, while the SSI framework strengthens decentralized identity management and data sovereignty—both aligning with the ethical and regulatory foundations of future 6G systems.

- **Cognitive Coordinator – NCSR** (Scores: 80%)

The Cognitive Coordinator ranked highly for its strategic role in orchestrating trust within adaptive 6G environments. As an AI-powered component, it interprets user trust intents—captured via the chatbot—and translates them into actionable system requirements. By coordinating five specialized Trust Functions, it ensures real-time alignment with user-defined trust goals. The result scored well in innovation level, strategic alignment with project goals, and feasibility, reflecting its importance in enabling explainable, user-centric AI behavior across SAFE-6G's architecture. Its integration potential within broader trust frameworks positions it as a key enabler of trustworthy 6G services.

Notable Emerging Assets

- **IMM's XR Applications: Factory and Formation Metaverse Apps** (Scores: 80–81%)

These extended reality (XR) applications stood out for their strong sustainability and feasibility, signalling the increasing relevance of immersive technologies in industrial and training contexts. Their alignment with DT and Industry 5.0 use cases suggests near-term applicability in manufacturing and collaborative engineering domains within the 6G ecosystem.

- **Privacy Mechanisms & SDP Functions** (Scores: 70–73%)

Although slightly lower in composite scores, assets such as eBOS's Software-Defined Perimeter SDP and SPACE Hellas's privacy-preserving modules remain essential to SAFE-6G's vision. These technologies bolster the trustworthiness layer by addressing critical aspects of user data protection,

AI compliance and ethical governance—key requirements for public acceptance and regulatory conformity in AI-powered telecom services.

This prioritization not only highlights high-impact technologies with near-market potential but also maps out a strategic landscape for coordinated exploitation across the consortium. The evaluation results serve as a blueprint for aligning technical development with commercialization efforts, stakeholder engagement and future R&D investment.

3.4.2 INSIGHTS AND NEXT STEPS

The results of this evaluation will directly inform the **Exploitation Roadmap**, identifying which assets are selected for:

- 1. Prioritizing High-Impact Assets for Immediate Action**
The consortium will focus on developing joint exploitation plans and pathways for the top-tier results, especially those ready for technology transfer by the end of the project.
- 2. Several assets—such as MLOps, differential privacy, explainable AI (XAI), and Software-Defined Perimeters (SDP)—can be combined into cohesive, privacy-centric AI toolkits tailored for telecom operators and industry verticals.** Likewise, XR-related outcomes can be integrated into immersive service platforms aimed at supporting Industry 4.0 use cases.
- 3. Developing Value Propositions Per Use Case Cluster**
Based on the project's verticals (e.g., smart factories, mobility, education), the consortium will map technology-to-business pathways, aligning exploitable results with specific stakeholder needs and return-on-investment models.
- 4. Engaging with External Stakeholders and Standards Bodies**
Joint dissemination and engagement efforts will be prioritized for high-ranking results, particularly those contributing to open standards, AI ethics and regulatory compliance, strengthening the project's impact at European and international levels.

3.5 JOINT EXPLOITATION

Following the identification and prioritization of key exploitable results, the SAFE-6G consortium has developed dedicated **Joint Exploitation Plans (JEPs)** for its two use cases:

- **Plan 1, Use Case 1: Industrial Metaverse of a Production Line**
- **Plan 2, Use Case 2: Metaverse for Education**

These plans outline collaborative exploitation strategies where multiple partners contribute interdependent technological components, domain expertise and market access to realize shared value propositions. Rather than pursuing isolated exploitation efforts, these joint plans promote synergy, enable integration across partner contributions and address end-to-end value delivery in well-defined 6G-enabled vertical scenarios.

Each JEP builds on a structured framework, beginning with a shared vision that defines the collective goal of the participating partners. This is followed by an analysis of synergies among the technologies

and competencies each partner brings to the table. The exploitation pathways and use case-specific impacts are then articulated to highlight market relevance, application potential and scalability.

To reinforce the strategic direction, each plan incorporates a Lean Business Model Canvas, which helps align partner roles and clarify the joint value proposition, customer segments, channels and revenue streams. Complementary strategic tools such as a SWOT analysis, Porter’s Five Forces framework and a Llava Matrix (for mapping technological integration and strategic alignment) provide a multidimensional view of the business and competitive landscape.

These joint exploitation plans serve as operational blueprints for future collaboration beyond the project lifecycle, supporting targeted commercialization, standardization contributions and coordinated dissemination to relevant market and policy stakeholders.

The following sections present a detailed overview of the two Joint Exploitation Plans developed within the SAFE-6G project: the first focuses on the Industrial Metaverse of a Production Line, while the second explores the Metaverse for Education. The next section provides an in-depth look at Joint Exploitation Plan 1, outlining the use case, mapping partner contributions, and detailing a coordinated strategy to translate SAFE-6G innovations into real-world industrial applications.

3.5.1 JOINT EXPLOITATION PLAN 1 – SAFE-6G USE CASE 1: INDUSTRIAL METAVERSE OF A PRODUCTION LINE

The SAFE-6G project focus on the next-generation communication networks, industrial digital transformation and the intelligent automation capabilities unlocked by advanced AI. Use Case 1, the Industrial Metaverse of a Production Line, serves as a high-impact scenario showcasing how 6G-enabled infrastructure, combined with trusted AI, immersive technologies and secure orchestration, can redefine the way industrial operations are monitored, managed and optimized.

A DT of an automated production line is at the core of this use case. This virtualized, real-time representation is enriched with a suite of SAFE-6G innovations, including intent-driven AI agents, XR-based human-machine interfaces and privacy-preserving, trust-aware orchestration layers. These components operate over a resilient and ultra-low-latency 6G core, enabling the seamless integration of cyber-physical systems and fostering real-time situational awareness, predictive maintenance and intelligent control loops.

The ambition of this JEP is to collaboratively translate these research outputs into concrete industrial capabilities. It aims to bridge the gap between technological development and industrial deployment by:

- Coordinating partner contributions around complementary assets such as the 6G core network stack (CUMUCORE), MLOps and XAI services (Eviden and Thales), intent classification chatbots (NCSR) and immersive metaverse applications (IMM).
- Defining clear exploitation pathways that map the SAFE-6G results to market-driven solutions addressing manufacturing automation, remote operations, worker training and factory resilience.

- Supporting joint value creation through shared IP strategies, co-branded demonstrators, standardization engagement and joint go-to-market initiatives.

This JEP also identifies the broader economic and societal impact of the Industrial Metaverse concept, particularly in enabling sustainable manufacturing, enhancing productivity through intelligent automation and empowering a skilled workforce via extended reality and AI-driven interfaces.

In the following subsections, the shared vision, partner synergies, exploitation pathways and strategic analyses (including Lean Business Canvas, SWOT, Porter's Five Forces and Llava Matrix) are presented to provide a comprehensive framework for the joint exploitation of SAFE-6G innovations within this use case.

3.5.1.1 SHARED VISION

Aligned with the overarching ambition of Joint Exploitation Plan 1, the vision behind Use Case 1: Industrial Metaverse of a Production Line is to establish a next-generation, interactive and autonomous industrial metaverse—a cyber-physical environment where machines, workers and decision-makers interact seamlessly through real-time data streams, immersive XR technologies and intelligent, intent-driven orchestration.

This envisioned environment aims not only to optimize operational efficiency but also to ensure resilience, trust and human-centric design. It embodies the SAFE-6G principles of secure and explainable AI, ultra-reliable communications and modular innovation tailored for industrial-scale adoption.

To turn this vision into reality, the joint exploitation strategy is centred on four strategic objectives, which directly reflect the combined contributions and technological assets of the involved partners:

- **Human-Centric Automation.** Empower factory personnel to interact directly with digital twins of their production lines using natural language through AI-powered chatbots. This facilitates intuitive control, real-time adaptation of processes and enhanced situational awareness for operators and managers.
- **XR-Augmented Decision-Making.** Leverage immersive XR interfaces and predictive analytics to support collaborative rescheduling, remote inspections and proactive maintenance—particularly under dynamic or unexpected operational conditions.
- **Distributed Trust Architecture.** Integrate cybersecurity, privacy-by-design, resilience and explainability features into the communication and orchestration layers. This ensures that all interactions—human or machine—are context-aware, secure and compliant with industrial governance policies.
- **Modular Deployment and Interoperability.** Deliver a flexible, modular suite of services and toolkits, including the 5G/6G core, CloudXR components, digital twin integration and trust-enabling middleware. These can be deployed independently or as a full-stack solution, depending on the digital maturity and transformation roadmap of the adopting industrial user.

This vision responds directly to the growing needs of modern manufacturing sectors for transparent, adaptive and secure infrastructures—needs that current legacy systems struggle to meet, particularly in scenarios demanding low latency, real-time collaboration and trusted AI integration.

3.5.1.2 SYNERGIES ACROSS PARTNERS

Building on the shared vision of a secure, intelligent and immersive industrial metaverse, Use Case 1 demonstrates the strategic value of orchestrated technological synergy across the SAFE-6G consortium. This joint effort brings together a multidisciplinary ecosystem of partners, each contributing critical components that align with four core functional layers: foundational connectivity, AI and trust enablers, user-centric interfaces and adaptive orchestration. Together, these components form a comprehensive and modular technology stack, designed for deployment in real-world manufacturing environments.

At the heart of this architecture lies the 5G/6G core network provided by CUMUCORE, which enables ultra-reliable low-latency communication (URLLC)—a fundamental requirement for real-time XR collaboration, predictive automation and seamless coordination between machines and human operators. This connectivity layer is critical incorporating advanced capabilities such as policy-based routing, adaptive QoS and continuous performance monitoring, thereby forming the digital systems of the industrial metaverses.

INF and NCSR, develop technical components that are closely related and a high collaboration between these can provide innovative results. The user-intent-driven chatbot guides non-expert users through a two-stage process, first classifying each query into one of five trust-function categories, then invoking a large language model with a tailored prompt to capture precisely the information the Cognitive Coordinator needs. The Cognitive Coordinator, an innovative, AI-powered orchestration component responsible for interpreting user trust intents and dynamically steering the system toward desirable, trustworthy operational states.

In this direction, Eviden's MLOps framework allows for the streamlined development, training and deployment of machine learning models across edge and cloud environments. These models enable predictive maintenance, dynamic scheduling and intelligent process adaptation. The framework enables operators to interact with digital twin systems using natural language commands—an intuitive step toward human-centric automation.

The trust and security layer is composed of several interlocking innovations. InQbit's Blockchain-based Self-Sovereign Identity (SSI) system ensures secure, verifiable identities and access control for all digital touchpoints within the factory. This is enhanced by smart contracts that govern audit trails and enforce policy compliance. Additional robustness is provided by Telefonica's Resilience Function and UNIWA's Trust Function, which detect and respond to anomalies, ensuring uninterrupted and secure operations even in the presence of failures or cyber threats.

Orchestration of these trust features is coordinated by NCSR's Cognitive Coordinator, a central policy engine that interprets user intent and orchestrates system-wide responses. For instance, in XR sessions involving sensitive design data, SPACE's Privacy Function is triggered to ensure strict data

minimization and controlled access. If deviations from expected system behaviour occur, InQbit's AI-driven Trust Agents adjust QoS levels or activate mitigation protocols in real time, preserving operational integrity.

Usability and human interaction are core priorities in the system architecture. Thales' XAI Assistant bridges the gap between complex AI decisions and end-users by delivering transparent, natural-language explanations—critical for trust and accountability. Meanwhile, IMM's CloudXR kit enables rapid deployment of immersive collaboration environments, allowing operators and engineers to experience and interact with digital twins in near real time. These capabilities are orchestrated by the Meta-Operating System developed by UPV, which coordinates the distributed services and monitors overall system health across edge-cloud resources.

Taken together, these elements constitute a cohesive, future-ready technological constellation. While each module holds standalone value, their collective integration offers a transformative solution for industrial environments seeking intelligent, secure and human-centric operations. This synergy reflects not only the technical strength of the consortium, but also its ability to align innovation with real-world industrial needs through coordinated exploitation.

3.5.1.3 EXPLOITATION PATHWAYS AND USE CASE IMPACT

Building on the shared vision and integrated partner synergies presented in previous sections, the exploitation strategy for Use Case 1: Industrial Metaverse of a Production Line is designed to transform SAFE-6G's technological innovations into market-ready, scalable solutions. This strategy takes a multi-layered approach, targeting a broad spectrum of stakeholders across the industrial value chain—from factory floor operators and IT departments to system integrators, equipment vendors and infrastructure providers.

At the core of this strategy is a modular adoption model. SAFE-6G components have been designed to function both as an integrated system and as standalone solutions. This flexibility allows industrial users to begin with a specific capability, such as a trusted communication layer, AI-based orchestration, or an XR interface and scale up over time based on operational needs and digital maturity.

Path 1: Product Development and Commercialization

Key SAFE-6G components—including the 5G/6G core, CloudXR kit, Meta-Operating System and various trust-enabling modules—are being prepared for commercialization. Partners such as IMM and CUMUCORE are well-positioned to lead the market introduction of plug-and-play XR connectivity kits and private 6G infrastructure solutions. These offerings may be distributed via licensing models, bundled service packages, or OEM integration for large-scale industrial clients.

Path 2: Service-Oriented Delivery Models

Software-based components such as the MLOps framework, Cognitive Coordinator, Trust Agents and resilience functions lend themselves to Software-as-a-Service (SaaS) delivery. These services can be layered on top of existing factory IT systems to enhance automation, explainability and compliance.

Path 3: Consulting, Integration and Demonstration Services

Recognizing that many industrial actors may lack in-house capabilities to deploy XR and AI technologies, partners such as **Telefonica** and **eBOS** will offer consulting, system integration and training services. Demonstrators built with the **CloudXR kit** will serve as **proof-of-concept platforms**, accelerating early-stage adoption and helping integrators and clients explore the industrial metaverse in action. This pathway is critical for **early market education** and trust-building in conservative sectors.

Path 4: Continued Research and Standardization

While several components are nearing market maturity, others—such as advanced explainability models, trust scoring under extreme conditions and semantic intent recognition—will benefit from further R&D. These topics form the basis for follow-up efforts in national and EU-funded programs related to 6G, AI trust and XR in industry. Additionally, partners like UPV and Telefonica will channel results into standards bodies (e.g., 3GPP, ETSI, IEEE), influencing future regulatory and interoperability frameworks.

Expected Impact

The impact of successfully exploiting Use Case 1 is multifaceted, delivering benefits across technological, industrial and societal domains:

- **For industrial actors**, the solutions bring enhanced reliability, greater operational efficiency and improved workforce safety through predictive automation, immersive interaction and trusted orchestration.
- **For technology providers**, the use case opens new business lines in XR-enhanced operations, AI-augmented factory orchestration and secure edge-cloud infrastructures tailored to industrial needs.
- **For society**, it promotes the ethical and responsible adoption of AI in one of the most critical economic sectors—manufacturing—thus contributing to long-term resilience, competitiveness and the green and digital transition in line with EU policy goals.

3.5.1.4 LEAN BUSINESS MODEL CANVAS

To better position the joint exploitation strategy of Use Case 1 within real-world industrial market conditions, the consortium applies the Lean Business Model Canvas. This framework provides a concise yet structured overview of how SAFE-6G's innovations translate into actionable business value, addressing user needs, defining delivery mechanisms and supporting sustainable growth.

1. Customer Segments

- **Primary:** Industrial manufacturers adopting digital twins, XR-based operator assistance, or AI-driven factory automation.
- **Secondary:** System integrators, industrial IT providers and consultancy firms focused on digital transformation and Industry 4.0/5.0 solutions.

2. Value Proposition

The SAFE-6G stack delivers a paradigm shift in how factories operate—merging **security, intelligence** and **immersive collaboration** through modular, trusted 6G infrastructure. Key value propositions include:

- Real-time XR-enabled collaboration and remote monitoring
- Predictive and adaptive operations via intent-driven AI and ML models
- Trusted, policy-aware orchestration ensuring privacy and resilience
- Scalable, decentralized 6G-ready infrastructure with low latency and high reliability

3. Channels

Market access will be achieved through a hybrid approach:

- Direct commercial offerings by partners (e.g., CUMUCORE, IMM)
- Joint demonstrators and pilots with early adopters, using the CloudXR kit and Meta-OS platform
- Licensing and SaaS delivery models for AI orchestration and trust components
- Consulting and integration services, especially for complex or multi-site deployments

4. Customer Relationships

The plan emphasizes **long-term, high-engagement relationships**, supported by:

- Dedicated technical support and integration assistance
- XR onboarding, training and usability workshops
- Iterative feedback loops during pilots for feature refinement and customization
- Partners such as Telefonica, InQbit and eBOS will lead client-facing services to ensure operational alignment and smooth adoption.

5. Revenue Streams

Multiple monetization pathways are anticipated, including:

- Sales of hardware kits (e.g., CloudXR-based deployment packages)
- Subscription-based access to AI orchestration and trust management tools
- Licensing of platforms such as OpenCAPIF and Meta-OS
- Customized consulting, training and systems integration projects

6. Key Resources

- Consortium-developed AI and orchestration software (MLOps, Trust Agents, Cognitive Coordinator)
- Industrial-grade 5G/6G network infrastructure
- Domain-specific expertise in XR, trust, security and privacy
- Demonstration and validation environments (e.g., XR testbeds, Meta-OS orchestration lab)

7. Key Activities

- Finalizing and packaging exploitable results for industrial deployment
- Executing pilot programs and collecting performance feedback

- Stakeholder education and dissemination through workshops and demonstrators
- Ongoing enhancement of modular components through real-world data and user input

8. Key Partnerships

- XR hardware and component suppliers
- Standardization and regulatory bodies (3GPP, ETSI, etc.) for compliance and adoption pathways
- Industrial early adopters engaged in co-validation and refinement
- Research institutions for continuous innovation and alignment with future 6G programs

9. Cost Structure

Primary cost drivers include:

- Final-stage R&D and integration for commercial readiness
- Pilot setup and evaluation in industrial environments
- Certification, security auditing and compliance alignment
- Production and maintenance of demonstration kits and XR hardware packages

This Lean Business Model Canvas complements the broader exploitation framework by mapping SAFE-6G's technical assets to sustainable commercial opportunities, anchored in industrial needs and supported by strategic partner collaboration.

3.5.1.5 SWOT ANALYSIS

The Industrial Metaverse envisioned in SAFE-6G Use Case 1 represents an action of XR, AI-driven orchestration and trust-enhanced 6G infrastructure. To assess the strategic positioning of this innovation within real-world industrial ecosystems, a structured SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis is presented below. This analysis directly supports the exploitation planning by identifying internal and external factors that influence SAFE-6G's path to market success.

Strengths

- **Technological Synergy and Modularity.** SAFE-6G brings together a diverse set of partner-developed innovations into a highly modular, interoperable architecture. The project's ultra-low-latency, secure 6G core provides a robust backbone for XR-based collaboration and AI-enabled digital twins, key capabilities for future industrial environments.
- **Human-Centric and Adaptable Interaction.** Unlike conventional automation platforms, SAFE-6G introduces cognitive adaptability through components like the Cognitive Coordinator and intent-based chatbots. These features allow real-time, natural language interaction between human users and systems, significantly improving usability, transparency and trust.
- **Scalability and Distributed Architecture.** Built on a cloud-edge continuum and orchestrated via the Meta-Operating System, the solution is inherently scalable—from localized deployments in small factories to global production networks—supporting a wide range of industrial scenarios.

Weaknesses

- **Integration Complexity.** The advanced nature of SAFE-6G's architecture, involving XR interfaces, AI models, trust functions and orchestration mechanisms, introduces **integration challenges**. Compatibility issues and technical bottlenecks may arise when deploying multiple interdependent modules in a live factory setting.

- **Limited Access to Industrial Data.** Many AI components rely on machine learning, which in turn requires access to operational data. However, **strict privacy, security and compliance regulations** in industrial settings often limit the availability and sharing of such data, slowing model training and optimization.
- **Sectoral Inertia and Adoption Barriers.** Heavy industry and highly regulated sectors may be reluctant to adopt AI or blockchain-enabled solutions due to **uncertainty, regulatory concerns and legacy system dependence**. Without strong proof-of-value and clear ROI, resistance to change could impede early adoption.

Opportunities

- **Rising Demand for Digital Twins and Predictive Maintenance.** Industry 4.0 adoption is accelerating, and digital twins, predictive maintenance and smart orchestration are at the forefront. SAFE-6G's human-centric, modular and secure approach directly aligns with this growing demand.
- **Remote Collaboration in High-Risk Sectors.** Fields such as aerospace, pharmaceuticals and energy increasingly require immersive, trusted and real-time remote collaboration—capabilities uniquely enabled by SAFE-6G's XR and AI-driven architecture.
- **Cross-Sector Scalability.** While validated in manufacturing, the SAFE-6G technology stack is applicable to other verticals including smart healthcare, logistics, infrastructure monitoring and public safety—broadening its market potential beyond the initial use case.

Threats

- **Proprietary Platforms and Market Consolidation.** A major external threat comes from large technology vendors developing vertically integrated, proprietary ecosystems that combine AI, XR, cloud and automation. These “walled garden” platforms could limit interoperability and discourage open, modular solutions like SAFE-6G.
- **Standardization Delays.** While the consortium is actively contributing to bodies like 3GPP, ETSI and IEEE, delays in industry-wide standards adoption could slow down regulatory acceptance and mainstream market integration.
- **Cybersecurity Landscape Volatility.** As SAFE-6G targets critical infrastructure, it will face ongoing risks associated with cyber threats, evolving attack vectors and shifting compliance requirements, potentially increasing costs, and deployment risks.

This SWOT analysis reinforces the strategic importance of SAFE-6G's approach—highlighting both its distinct market advantages and areas that require mitigation through thoughtful planning, strong partner coordination and continued research investment.

3.5.1.6 PORTER'S FIVE FORCES FRAMEWORK

To complement the internal strategic assessment provided by the SWOT analysis, Porter's Five Forces Framework is applied to evaluate the external market dynamics and competitive pressures that could impact the successful deployment and scaling of Use Case 1: Industrial Metaverse of a Production Line. This analysis offers a structured view of industry attractiveness and SAFE-6G's potential to establish a defensible market position.

1. Threat of New Entrants – Risk: Moderate. The industrial metaverse remains a relatively nascent and specialized domain. The technical depth, system-level integration, and trust-sensitive architecture of SAFE-6G create significant barriers to entry. However, large technology players—especially cloud infrastructure providers and robotics manufacturers—possess the resources and market reach to

enter this space quickly. Continued focus on standardization, modularity and open collaboration will be essential to maintain differentiation.

2. Bargaining Power of Suppliers – Risk: Low. SAFE-6G benefits from a highly modular architecture, drawing on interoperable components across XR, AI, privacy and 6G connectivity domains. This flexibility allows for substitution and sourcing from multiple vendors, reducing lock-in and dependency on any single supplier. The consortium’s ability to integrate diverse technologies ensures resilience in sourcing and supply chain adaptability.

3. Bargaining Power of Buyers – Risk: Moderate to High. Industrial buyers—especially large manufacturers—typically possess strong negotiation leverage due to high-value contracts and the need for customized, mission-critical solutions. However, SAFE-6G mitigates this risk by offering a standards-compliant, modular solution that can scale from SMEs to multinational factories. This adaptability enables the consortium to address a wide range of buyer needs while maintaining manageable cost structures.

4. Threat of Substitutes – Risk: Moderate. Legacy systems such as SCADA and PLC-based automation remain entrenched in many factories. While mature, these technologies lack immersive capabilities, AI-enhanced orchestration and integrated trust layers. Competing digital twin platforms may offer partial functionality but do not yet provide SAFE-6G’s holistic stack—especially regarding intent recognition, explainability and policy-driven trust orchestration.

5. Industry Rivalry – Risk: High. The market for industrial XR, AI and automation is becoming increasingly competitive, with multiple research consortia and commercial players exploring Industry 4.0/5.0 and metaverse-aligned solutions. However, SAFE-6G distinguishes itself through its unique fusion of trusted AI, explainable orchestration, modular 6G connectivity and immersive interfaces. This integrative approach offers a more complete and extensible solution than most current offerings.

Overall, while competitive pressures exist, especially from large incumbents and emerging substitutes, SAFE-6G is strategically positioned to compete through technological differentiation, scalable modularity, and human-centric trust architecture. These advantages provide a solid foundation for securing market share in the evolving industrial metaverse landscape.

3.5.1.7 LLAVA MATRIX ANALYSIS: MAPPING ALIGNMENT AND INTEGRATION

To complement the prior strategic assessments, the Llava Matrix offers a multidimensional perspective on how SAFE-6G’s technological components align with user needs, operational contexts, and long-term strategic goals. Unlike traditional technology roadmaps, the Llava Matrix explicitly maps capabilities to impact—assessing how each innovation contributes to key factors such as performance, trust, decision-making and system resilience.

User Needs and Operational Context

In the industrial metaverse environment envisioned for Use Case 1, users such as production engineers, machine operators and safety managers require tools that support:

- Real-time visualization and situational awareness
- Intuitive and secure control over automated processes
- Dynamic adjustment of production flows
- Assurance of privacy, system integrity and safety

SAFE-6G responds to these needs through an array of modular, user-centric tools, including:

- A chatbot interface for intent-driven interaction
- XR-guided DT manipulation
- Trust orchestration functions that adapt network behaviour to the user's operational context and risk level

Technology-to-Capability Alignment

The Llava Matrix illustrates how specific technological components directly support key operational and strategic needs:

- **Cognitive Coordinator + Blockchain SSI.** Links user intent to quantifiable trust levels and dynamically orchestrates system behaviour (e.g., enforcing privacy or resilience policies) based on real-time context.
- **Meta-Operating System + MLOps.** Enables efficient deployment and lifecycle management of AI models at the **edge or in the cloud**, optimizing resource use and enabling context-aware intelligence.
- **OpenCAPIF + API Gateways.** Facilitates secure, standardized service exposure and interaction between trust agents, XR systems and orchestration layers—enabling seamless component integration and policy enforcement.
- **Explainable AI + XAI Assistant** Translates complex system performance and trust metrics into **human-readable insights**, improving transparency and building end-user confidence in AI-driven automation.

Strategic Value Streams

The Llava Matrix also clarifies how SAFE-6G supports broader industrial and technological transformation:

- Trustworthy Autonomy. Operators can safely delegate routine or complex tasks to AI systems while maintaining control, thanks to **transparent interfaces** and **policy-based trust coordination**.
- Scalable Intelligence. The system learns from historical actions—stored immutably via **smart contracts** and adapts over time, delivering increasingly **resilient, explainable, and efficient** performance.
- Cross-Layer Synchronization. From network infrastructure to user interfaces, each layer of SAFE-6G responds cohesively to system changes, ensuring **low-latency, context-aware behaviour** with minimal inconsistency or lag.

Emergent Gaps and Insights

While the Llava Matrix underscores the strengths of SAFE-6G’s architecture, it also reveals areas that warrant further attention:

- **Interoperability challenges** remain, especially when integrating with legacy systems or vendor-locked industrial hardware. Ensuring cross-platform compatibility will require additional abstraction layers or middleware.
- **Behaviour under stress or failure conditions**, such as partial network outages or simultaneous triggering of multiple trust functions—requires more robust arbitration logic. Coordination across privacy, resilience and safety modules must rely on a shared temporal framework, which is still under development.
- **Human factors** in XR deployment must also be addressed. Real-world adoption in factory settings requires careful attention to ergonomic design, safety compliance and digital readiness of the workforce. SAFE-6G must ensure its XR toolkits—such as the CloudXR kit—are not only technically sound, but also user-friendly, safe, and adaptable to diverse work environments.

In summary, the Llava Matrix affirms SAFE-6G’s holistic alignment between technology, user experience and strategic industrial needs, while also guiding the next steps for integration, validation, and user-centric refinement. It provides a valuable reference point for ongoing development, market preparation and cross-sector scalability of the SAFE-6G framework.

3.5.1.8 CONCLUSION

The Joint Exploitation Plan for Use Case 1: Industrial Metaverse of a Production Line demonstrates how the SAFE-6G project delivers a forward-looking, modular, and trust-centric approach to transforming industrial operations. By leveraging a diverse yet integrated technology stack—including 6G core connectivity, AI-driven orchestration, XR-enabled DTs and privacy-preserving trust functions—the consortium is positioned to address the complex demands of next-generation manufacturing.

Through strategic tools such as the Lean Business Model Canvas, SWOT analysis, Porter’s Five Forces and the Llava Matrix, this exploitation plan articulates not only the technological and market potential of SAFE-6G innovations, but also the operational pathways for real-world deployment. It identifies key stakeholders, revenue models, risks, and opportunities, while aligning with the evolving digital transformation agendas across industrial sectors.

The modularity and interoperability of the SAFE-6G ecosystem enable flexible adoption scenarios—from targeted integration of XR interfaces or AI toolkits to full-scale deployment of a secure, intelligent, and immersive production environment. Moreover, the plan outlines multiple commercialization avenues, including product development, SaaS offerings, consulting services and continued research contributions.

Looking ahead, the focus will be on consolidating technical readiness, validating solutions through pilot deployments, and engaging early adopters through co-innovation. SAFE-6G’s commitment to

open standards, ethical AI and scalable trust architectures ensures its long-term relevance and adaptability in a competitive and fast-evolving industrial landscape.

In conclusion, Use Case 1 not only exemplifies the transformative impact of SAFE-6G technologies but also lays a solid foundation for industrial metaverse adoption—turning advanced research into actionable, high-value innovation.

3.5.2 JOINT EXPLOITATION PLAN – SAFE-6G USE CASE 2: METAVERSE FOR EDUCATION

Building on the foundations of Joint Exploitation Plan 2, Use Case 2: Metaverse for Education explores how SAFE-6G technologies can be applied to transform the educational landscape through immersive, intelligent, and secure learning environments. This scenario focuses on deploying XR-enhanced teaching spaces powered by AI-driven content adaptation, real-time feedback, and trusted communication infrastructure.

The goal is to create personalized and interactive learning experiences that are resilient, accessible, and scalable, addressing both remote and hybrid education models. From vocational training and university-level STEM programs to corporate upskilling and safety instruction, this use case has broad applicability and strong societal impact potential.

The educational metaverse scenario leverages key SAFE-6G components in novel ways:

- CloudXR kits and immersive classroom interfaces for collaborative, hands-on learning.
- Explainable AI systems that adapt content in real time based on student performance and preferences.
- SSI and privacy-preserving orchestration for ethical and compliant use of learner data.
- High reliability 6G infrastructure to support synchronous multi-user XR environments across geographies.

The Joint Exploitation Plan for Use Case 2 outlines how consortium partners will co-develop and position these solutions within the **education technology (EdTech)** sector. It also maps exploitation activities to stakeholders including:

- Educational institutions and training centres
- Government and EU-funded digital education initiatives
- XR content developers and e-learning platforms
- IT integrators and academic research labs

The following sections detail the shared vision, synergies among partners, exploitation pathways and strategic analyses for this use case, highlighting how SAFE-6G can redefine the future of education through innovation rooted in trust, interactivity, and intelligent connectivity.

3.5.2.1 SHARED VISION

SAFE-6G Use Case 2 envisions a transformative leap in the field of digital education—one where immersive experience, real-time collaboration and human-centric trust frameworks converge to redefine how teaching and learning are delivered and experienced. Responding to the accelerated shift toward hybrid and remote learning, further catalysed by the COVID-19 pandemic, this use case reimagines the classroom as an intelligent, persistent, and inclusive metaverse. The initiative is led by IMM, with contributions from a multidisciplinary consortium committed to making education more accessible, adaptive, and secure on a global scale.

At the core of this vision lies the concept of a hybrid metaverse learning environment, where both remote and in-person participants coexist within a spatially aware, XR-enabled space. Here, students and educators engage not just through screens, but through immersive interfaces, real-time AI-driven feedback and dynamic adaptation based on each learner’s behaviour, intent, and contextual needs. This environment is not a mere replication of physical classrooms—it is a pedagogical enhancement: enriched with personalized content, explainable AI support and a resilient infrastructure that prioritizes equity, trust, and continuity.

The exploitation vision supporting this use case is built around four primary objectives:

- **Empower Hybrid Learning.** Provide an immersive and persistent digital space that supports real-time collaboration among students, teachers and learning materials. This goes far beyond traditional video conferencing by enabling shared spatial awareness, virtual object manipulation and multi-user co-presence through XR.
- **Enable Personalized Support through AI.** Use natural language chatbots, intent recognition and explainable AI to tailor content delivery in real time. Educators can dynamically adjust session pacing and focus, while learners receive contextual support through conversational agents embedded in the virtual learning environment.
- **Establish a Trust-Enabled Infrastructure.** Integrate SAFE-6G’s trust mechanisms—including privacy-preserving computation, SSI-based identity verification and resilient network orchestration—into the educational platform. These features ensure secure and ethical handling of sensitive learner data throughout the learning process.
- **Promote Interoperability and Scalability.** Support a wide range of devices, learning content formats and deployment contexts—whether in schools, universities, or corporate training centres. Modular design allows institutions to adopt SAFE-6G technologies incrementally, depending on digital maturity, policy goals and available resources.

This shared vision responds to a global challenge: existing e-learning platforms and XR applications fall short in delivering personalized, secure, and high-performing hybrid education. SAFE-6G addresses this gap by combining high-bandwidth, low-latency connectivity with AI-based orchestration and trust-centric design—offering a truly next-generation alternative to traditional learning management systems (LMS) and videoconferencing tools.

The deployment strategy supports multiple adoption tracks:

- **Software Licensing and SaaS Delivery.** Core components—such as AI chatbots, the Cognitive Data Coordinator and privacy orchestration modules—can be licensed individually or accessed

via SaaS. These tools are compatible with existing LMS or XR platforms, offering plug-in integration with minimal disruption.

- **Hardware-Software Integration via XR Kits.** MM’s CloudXR Kit for education offers a ready-to-use package that combines hardware, pre-configured software, and orchestration logic. It supports rapid deployment for pilots, training programs, or institutional testing.
- **Consulting and Transformation Services.** Specialized consortium partners will offer consulting support for integration, digital readiness assessment, faculty onboarding and long-term sustainability planning. This enables institutions to adopt the SAFE-6G stack with confidence, even without deep technical expertise.

Ultimately, SAFE-6G’s educational metaverse is not only a technological evolution—it is a response to societal imperatives for resilient, inclusive, and ethically grounded learning ecosystems. By embedding XR, AI and trust infrastructure into the core of digital education, SAFE-6G offers a scalable, future-ready framework that empowers institutions, educators, and learners alike.

3.5.2.2 SYNERGIES ACROSS PARTNERS

Use Case 2 of the SAFE-6G project—centred on the development of a metaverse for education—benefits from a uniquely diverse and complementary network of partner synergies. While each organization contributes a specialized technology or function, the true value emerges through cross-layer integration that spans infrastructure, AI orchestration, trust enforcement and immersive human-machine interaction.

Infrastructure Layer: Ultra-Reliable Connectivity

At the foundation lies the next-generation 5G/6G core network developed by CUMUCORE, providing ultra-low latency and deterministic performance—both essential for immersive, XR-based educational sessions. These hybrid learning environments, which blend co-located and remote participants, demand highly responsive bandwidth management and strict latency guarantees. CUMUCORE’s software-defined RAN (SW-RAN) and programmable network functions enable real-time orchestration of these connectivity requirements, setting the stage for seamless user experience.

Edge-Cloud Orchestration and AI Integration

Building on this infrastructure, UPV’s Meta-Operating System (Meta-OS) orchestrates compute, network and trust resources dynamically across edge and cloud domains. In educational contexts—where device diversity, variable session loads and changing user behaviours are the norm—this orchestration ensures performance, scalability and efficiency.

In parallel, Eviden’s MLOps framework enables intelligent management of AI services powering the learning environment. AI models used for personalization, engagement tracking, and feedback generation are efficiently trained, deployed and updated in real time. Together, Meta-OS and MLOps provide the backbone for AI-enhanced adaptive learning.

Interaction and Experience Layer: Enabling Human-Centric Learning

At the user interaction level, powerful synergies emerge between **NCSR**D, **INF**, **IMM** and **THALES**:

- **NCSR**D’s **Cognitive Coordinator** and **intent classification chatbot** translate voice or text commands from users into system-level actions, enabling learners and instructors to intuitively interact with the platform.
- **INF**’s **conversational interface** extends these capabilities into active learning scenarios, where students can request additional support, content clarification, or custom explanations—fostering deeper engagement.
- **THALES**’s **XAI Assistant** ensures transparency by explaining the rationale behind system decisions. This is especially important for non-technical users, enhancing **trust and interpretability** in the learning process.

Leading the implementation, IMM contributes its CloudXR Kit and Sharing XR platform—a immersive learning solution enabling persistent, collaborative XR classrooms. These platforms support spatial content manipulation, multi-user interaction and rapid deployment for pilot programs, demos, or cross-border educational exchanges.

Trust and Security Layer: Ethical Foundations and Resilience

The trust layer, a defining aspect of SAFE-6G, integrates critical components:

- **eBOS**’s **SDP-enabled Safety Function**, **SPACE**’s **Privacy Function**, **Eviden**’s **Self-Sovereign Identity (SSI)** and **InQbit**’s **blockchain-based credentialing** form a cohesive framework for secure authentication, role-based access, privacy-preserving data sharing and auditable interactions. These are dynamically managed by the Cognitive Coordinator, ensuring trust adapts to user roles, session contexts and location.
- **Telefonica**’s **OpenCAPIF framework** enables secure API exposure and service discovery across SAFE-6G elements and external platforms (e.g., LMS, biometric tools, video libraries). This promotes interoperability and extensibility, allowing educational institutions to integrate the system into their existing digital infrastructure.
- **UNIWA**’s **Resilience Function** ensures session stability under fluctuating loads or partial failures. It interfaces with Meta-OS and MLOps to maintain quality of experience through real-time performance assessment, failover strategies and graceful degradation—especially important during critical sessions such as exams or assessments.
- **SPACE** and **Eviden**’s **trust components** also anchor the system’s ethical and legal compliance. Learners maintain full control over personal and biometric data, with privacy settings enforced via SSI and contextual consent protocols. These features reflect the consortium’s commitment to protecting user autonomy and digital rights.

Integrated Impact

Together, these elements form a deeply interconnected and human-centric solution stack. SAFE-6G’s educational metaverse is not just a technology platform—it is a trust-driven, adaptive, and inclusive learning ecosystem. Each partner’s contribution is amplified through strategic interdependencies, from infrastructure to experience to governance.

This collaborative architecture positions Use Case 2 as a reference model for the future of digital education—combining performance, security, and pedagogical innovation. As education systems

worldwide face increasing demands for flexibility, personalization, and equity, SAFE-6G offers a compelling, scalable and ethical response.

Case 2 of the SAFE-6G project—focused on the development of an educational metaverse—benefits from an exceptionally rich and diverse network of synergies among project partners. Each partner brings a specialized technological innovation or functional capability, but their true value emerges through seamless orchestration across layers: from infrastructure and AI orchestration, to trust enforcement, human-machine interaction, and immersive learning tools.

At the **infrastructure level**, **CUMUCORE** provides the cornerstone: a next-generation 5G/6G core network with ultra-low latency and real-time responsiveness, which is critical for XR-based educational sessions. The hybrid nature of these sessions—merging co-located and remote participants—requires dynamic bandwidth allocation and latency guarantees that only a programmable, software-defined 6G architecture can offer. CUMUCORE's SW-RAN capabilities and deterministic network functions lay the foundation for all higher-layer services, enabling immersive collaboration without perceptible lag.

UPV adds orchestration power through the **Meta-Operating System**, which allocates compute, trust, and connectivity resources intelligently across edge and cloud. This is key for educational environments, which are highly variable in terms of user load, device heterogeneity and time-of-day demand. Combined with Eviden's **MLOps framework**, the system ensures that AI models (e.g., for personalization, interaction analysis and real-time feedback) are trained, deployed, and maintained efficiently. This combination ensures that every XR classroom is powered by continuously learning AI services, dynamically orchestrated for performance and cost-effectiveness.

At the **interaction layer**, synergies arise between **NCSR**, **INF**, **IMM** and **THALES**. NCSR's **Chatbot** and **Cognitive Coordinator** work in tandem to translate student and instructor commands into network actions—such as boosting privacy, adjusting session permissions, or invoking explainable feedback from XR agents. INF's **intent-driven chatbot app** extends this capability into a full conversational interface that supports active learning: students can request clarifications, content replays, or topic-specific discussions, all delivered via intelligent, natural-language interfaces.

THALES's XAI assistant enhances transparency. By integrating with the chatbot, it allows users—especially those unfamiliar with AI or network configurations—to understand how system decisions are made. For example, if privacy levels are increased mid-session due to new participants joining, XAI explains the rationale in intuitive terms, reinforcing trust in the platform. These tools form a powerful triad that facilitates trust-by-design, transparency, and user empowerment in digital learning.

IMM, the use case leader, supplies the **CloudXR kit** and the **ShariingXR platform**, which together offer a ready-to-use immersive learning system. The CloudXR kit and ShariingXR ensure portability and ease of deployment—vital for demos, pilot programs, and cross-border educational outreach. When integrated with SAFE-6G's trust enablers and network functions, these platforms represent a solution for educational institutions seeking to adopt XR-based hybrid teaching.

The **trust layer** is where SAFE-6G's synergies achieve their highest impact. **eBOS's SDP-enabled Safety Function, SPACE's Privacy Function, Eviden's SSI system** and **InQbit's blockchain-based credentialing** form a coherent suite of trust enforcement components. Together, they handle secure user identification, role-based access control, privacy-preserving content sharing and auditability of interactions. These functions are dynamically orchestrated by the Cognitive Coordinator, ensuring adaptive trust management depending on who is accessing the system, from where and under what context.

Telefonica's OpenCAPIF framework underpins secure and standardized API access across this diverse ecosystem. In a metaverse education context, OpenCAPIF enables third-party LMS platforms, video libraries, biometric sensors, or even exam proctoring tools to connect securely and contextually to SAFE-6G resources. This promotes openness and extensibility—crucial for real-world adoption where institutions rely on diverse, evolving tech stacks.

UNIWA's Resilience Function plays a vital role in maintaining consistent user experience, especially under fluctuating user loads or partial system failures. Its integration with MLOps and Meta-OS ensures real-time performance assessment, dynamic failover strategies and graceful degradation—all of which are critical in ensuring that educational activities are never disrupted, especially during high-stakes sessions like exams or thesis defences.

Lastly, **SPACE's Privacy Function** and **Eviden's SSI component** anchor the ethical and legal foundations of the educational metaverse. They enable student data (including biometric or behavioural information) to be used only with explicit, contextual consent and ensure that learners retain control over their digital identity and personal information. These functions are not simply technical add-ons—they reflect the consortium's commitment to safeguarding the rights, dignity, and autonomy of users in digital learning environments.

In sum, the consortium for Use Case 2 operates as an interlinked system of innovation, with each partner's contribution amplified through strategic interdependencies. SAFE-6G's educational metaverse is not merely a sum of its parts; it is an integrated, human-centric framework—designed for reliability, inclusivity, trust, and educational excellence. This powerful synergy positions the use case as a reference model for next-generation digital learning ecosystems in Europe and beyond.

3.5.2.3 EXPLOITATION PATHWAYS AND USE CASE IMPACT

Building on the technological synergies detailed in the previous section, the exploitation strategy for Use Case 2: Metaverse for Education is focused on translating SAFE-6G's innovations into sustainable, modular, and scalable solutions for the education and corporate training sectors. This strategy recognizes that the future of learning lies not only in digitization but in secure, immersive, and intelligent virtualization, where learning experiences are both personalized and trusted.

The SAFE-6G educational metaverse introduces a paradigm shift—replacing static content and traditional video-based e-learning with dynamic, XR-driven, hybrid environments. These spaces allow geographically distributed learners and educators to collaborate in real time, interact through shared

virtual content, and dynamically adjust session parameters such as privacy, access and pedagogical focus.

To translate this potential into tangible impact, the joint exploitation strategy follows multiple complementary pathways:

Path 1: Modular Technology Commercialization

Key SAFE-6G components such as the Cognitive Coordinator, Privacy Function, Chatbots and XAI assistant will be packaged as modular services for integration into third-party platforms, including existing Learning Management Systems (LMS) and XR training apps. These components support plug-and-play functionality and can be deployed either independently or as part of a holistic digital learning environment. For example, a university could adopt the intent-based chatbot as a first step, then progressively integrate trust orchestration and privacy personalization tools as its infrastructure matures.

This modular model is ideal for academic institutions, EdTech companies and training providers seeking targeted enhancements without full system replacement. It allows stakeholders to address specific pain points—like real-time feedback, adaptive scheduling, or user-centric data control—while maintaining flexibility and minimizing upfront investment.

Path 2: SaaS Delivery of Intelligent Trust Frameworks

The SAFE-6G trust infrastructure—including the Resilience Function, Safety Function, and Blockchain-based SSI system—could potentially be delivered as cloud-based SaaS offerings. Educational institutions will be able to subscribe to services that ensure secure content sharing, persistent identity verification, dynamic session continuity and compliance with evolving data privacy regulations (e.g., GDPR, FERPA). These features are especially critical in multi-tenant metaverse classrooms, where student data must be kept secure and educational resources protected from unauthorized access or misuse.

Path 3: Consulting and Digital Transformation Services

Given the relative novelty of XR and 6G technologies in the education sector, adoption is often hindered by a lack of internal technical capacity. To bridge this gap, consortium members such as Telefonica, eBOS and NCSR D will offer specialized consulting services. These include infrastructure assessments, digital transformation roadmaps and tailored integration plans to help schools, universities, and vocational institutes onboard SAFE-6G components in alignment with their goals.

Workshops, training sessions and capacity-building programs will also be offered to ensure that educators, IT staff and administrators can operate and evolve the system post-deployment.

Path 4: Research Continuity and Standardization Contributions

Several components developed under Use Case 2—especially the privacy-aware trust functions, intent classifiers, and SSI systems—are at the frontier of technological maturity. These elements will benefit from continued refinement through follow-up research initiatives, especially under European and national calls related to 6G, AI in education, or data ethics.

Moreover, SAFE-6G partners such as UPV and Telefonica will channel their results into standardization efforts at bodies like 3GPP, ETSI and IEEE, helping to shape the future landscape of educational metaverse interoperability, data governance and trust.

Expected Impact

The outcomes of Use Case 2 will generate value across multiple stakeholder groups and domains:

- **For Educational Institutions:** A seamless hybrid learning experience that enhances engagement, supports personalized instruction, and safeguards sensitive student data. The SAFE-6G framework will enable more inclusive and resilient education—particularly important in rural areas, disaster recovery scenarios, or during future public health disruptions.
- **For Technology Providers:** A rich opportunity to commercialize modular, standards-aligned tools that meet growing demand for secure, interactive educational environments. This includes both B2B (learning platforms, hardware vendors) and B2G (government education programs) channels.
- **For Learners and Instructors:** A more interactive, intuitive, and trustworthy learning journey. XR engagement, conversational AI and adaptive privacy controls improve student motivation and confidence while reducing instructor overload.
- **For Society:** A significant step toward democratizing access to high-quality education. SAFE-6G lowers the digital divide by providing scalable and secure infrastructure for virtual learning, addressing both economic and geographic inequalities.

3.5.2.4 LEAN BUSINESS MODEL CANVAS

The SAFE-6G Metaverse for Education delivers a future-ready platform tailored for hybrid and immersive learning. The Lean Business Model Canvas for Use Case 2 captures how SAFE-6G's innovations align with the needs of real-world education ecosystems and how they can be sustainably commercialized and scaled.

Customer Segments

The SAFE-6G educational metaverse targets a multi-tiered ecosystem of users and stakeholders:

- **Primary:** Educational institutions (universities, schools, vocational training centers) seeking to modernize hybrid learning environments through immersive technologies.
- **Secondary:** Corporate learning and development departments interested in scalable, secure and personalized training platforms.
- **Tertiary:** Public agencies and governments promoting digital literacy, lifelong learning, or pandemic preparedness in education.
- **Early adopters:** Tech-forward institutions, EdTech platforms, XR content providers and research universities with existing 5G/6G pilot initiatives.

These customer segments are united by common pain points—fragmented digital tools, limited interactivity, privacy concerns and sub-optimal learning outcomes in remote or hybrid settings.

Value Propositions

SAFE-6G offers a differentiated and holistic solution that addresses the unmet needs of hybrid learning environments:

- **Immersive Learning Spaces:** XR-based persistent classrooms that merge real and virtual collaboration for learners and teachers, enhancing engagement and comprehension.
- **AI-Powered Personalization:** Adaptive learning environments driven by conversational agents, intent recognition and explainable AI that react to learner behaviour and preferences.
- **Security and Trust at the Core:** Data protection, dynamic privacy management and resilient service orchestration embedded across the infrastructure.
- **Interoperability with Legacy Systems:** Modular architecture that supports phased adoption and integration with existing LMS, XR hardware and IT environments.
- **Cost-Efficient Demonstration and Scaling:** Via CloudXR kits and SaaS trust functions, stakeholders can evaluate and adopt components progressively without large upfront investment.

Together, these elements enable a future-ready educational infrastructure that prioritizes inclusivity, safety, and learner autonomy.

Channels

The delivery of SAFE-6G educational solutions will leverage a combination of direct and indirect outreach methods:

- **Direct Sales:** Through consortium partners offering turnkey solutions (e.g., IMM’s CloudXR kit, Telefónica’s orchestration services).
- **Partner Distribution:** Through EdTech vendors and system integrators embedding SAFE-6G components into broader digital learning solutions.
- **Pilots and Demos:** Public and private partnerships to showcase the immersive metaverse learning experience in real institutions.
- **SaaS and Cloud Platforms:** Secure AI functions and trust services available via web-based portals with subscription models.
- **Public Procurement:** Engagement with education ministries and local authorities to integrate solutions into national digital education programs.

These channels will be used strategically to balance visibility, reach and operational cost-efficiency.

Customer Relationships

SAFE-6G’s deployment in education demands high-trust, high-touch relationships:

- **Tailored Onboarding and Training:** Institutions will receive hands-on support for deploying XR and AI tools, adapting them to specific curricula, user needs and IT constraints.
- **Ongoing Support Services:** Remote troubleshooting, updates and performance optimization provided through consortium partners.

- **Feedback-Driven Iteration:** AI-driven analytics and user surveys will feed into continuous product refinement cycles.
- **Community Engagement:** Creation of knowledge-sharing communities (e.g., forums, webinars, sandbox environments) for educators and IT teams adopting the platform.

These relationships will be essential for building confidence in immersive, AI-powered learning technologies.

Revenue Streams

SAFE-6G partners will pursue diversified revenue models tailored to customer needs and deployment contexts:

- **One-Time Product Sales:** CloudXR kits and initial software licenses (e.g., chatbots, privacy functions) for institutions seeking full on-premises control.
- **Subscription Services:** Monthly or annual fees for AI orchestration, real-time trust management and SaaS-based privacy systems.
- **Tiered Access Models:** Variable pricing for small schools, large universities and corporate clients based on features, number of users and level of customization.
- **Consulting and Integration Services:** Professional services for system configuration, training, change management and regulatory compliance.
- **R&D and Public Funding:** Co-financing from national and EU programs for continued research, piloting, and dissemination efforts.

This blend ensures resilience against budget cycles and provides flexibility across different institutional capacities.

Key Resources

To deliver on its value propositions, SAFE-6G will leverage a rich portfolio of resources:

- **Core Technological Assets:** 5G/6G core (CUMUCORE), Privacy Function (SPACE), SSI (Eviden/InQbit), Cognitive Coordinator (NCSR), XR applications (IMM).
- **AI Models and Data Infrastructure:** MLOps framework, XAI assistant, intent classifiers and synthetic + real datasets.
- **Physical Demonstrators:** CloudXR kits and immersive demo labs that showcase the full SAFE-6G stack.
- **Domain Expertise:** In education technology, human-machine interaction, data ethics, network architecture and immersive learning.
- **Network of Partners:** Trusted relationships across academia, industry, and public institutions to support dissemination and feedback loops.

These resources are foundational to not just deployment, but long-term scalability and innovation.

Key Activities

The SAFE-6G consortium will focus its operational efforts on:

- **Component Finalization:** Ensuring the readiness, usability, and compliance of all exploitable results for educational contexts.

- **Integration Testing:** Validating interoperability across XR devices, AI modules, trust services and distributed network components.
- **Pilot Deployments:** Real-world implementation in educational environments to demonstrate impact and gather performance feedback.
- **User Training and Enablement:** Developing toolkits, documentation and training programs for educators, IT staff and decision-makers.
- **Regulatory Engagement:** Ensuring privacy, safety and accessibility standards are met or exceeded to encourage institutional buy-in.

These activities align closely with pathways to commercialization and standardization.

Key Partnerships

The exploitation of Use Case 2 will be amplified by:

- **XR Hardware Providers:** To deliver compatible and cost-effective immersive devices for classrooms and learners.
- **Education Ministries and Agencies:** To support scaled adoption and integration into national education strategies.
- **EdTech Integrators:** For embedding SAFE-6G capabilities into broader digital learning ecosystems.
- **Standardization Bodies:** (e.g., ETSI, IEEE, 3GPP) to drive compliance and future-proofing.
- **Academic and Industry Collaborators:** For joint research, dissemination, and training program development.

Strong partnerships will also facilitate cross-sector applications, from K-12 to vocational training and corporate upskilling.

Cost Structure

Key cost drivers for Use Case 2 include:

- **R&D and Customization:** Final development of components for educational scenarios, adaptation to diverse pedagogical needs.
- **Pilot Implementation:** Cost of hardware kits, network deployment and user support for demo sites.
- **Data Collection and Annotation:** For improving AI models and aligning them with real-world classroom behavior and expectations.
- **Standardization and Certification:** Ensuring SAFE-6G meets compliance requirements for public and private sector use.
- **Marketing and Dissemination:** Producing promotional materials, attending conferences and hosting stakeholder engagement events.

These investments are critical for reaching early adopters, validating value, and paving the way for mass adoption.

3.5.2.5 SWOT ANALYSIS

The Metaverse for Education under SAFE-6G represents a groundbreaking intersection of immersive XR environments, AI-driven personalization, and secure, trust-by-design network infrastructure. This

SWOT analysis evaluates the internal capabilities and external market conditions that shape the strategic positioning of this use case in the evolving education and EdTech landscape.

Strengths

- **Human-Centric Immersive Learning Architecture.** SAFE-6G offers a next-generation hybrid classroom environment that emphasizes inclusiveness, interactivity, and learner engagement. Through the fusion of XR, AI personalization and conversational agents, the platform enhances user experience well beyond conventional e-learning formats.
- **Trust-by-Design Infrastructure.** Unlike retrofitted solutions, SAFE-6G embeds trust from the ground up. Integrated privacy enforcement, SSI and context-aware trust orchestration ensure compliance with privacy regulations while promoting ethical digital learning environments.
- **Modular and Interoperable Architecture.** SAFE-6G supports phased, component-based adoption, allowing institutions to integrate chatbot interfaces, privacy layers, or immersive XR systems based on readiness and infrastructure maturity. This flexibility lowers adoption barriers and supports gradual transformation.
- **AI-Driven Adaptability.** Conversational AI and intent classifiers dynamically adapt system behavior to learner needs—adjusting privacy, content delivery and access in real time. These features simplify user experience and mitigate the technical complexity often associated with immersive learning.
- **Deployment-Ready Demonstrators.** The availability of **IMM’s CloudXR kit** and **ShariingXR platform** allows consortium partners to deliver plug-and-play immersive environments. These demonstrators facilitate early engagement, stakeholder buy-in and rapid proof-of-concept validation in real-world settings.

Weaknesses

- **Integration Complexity.** The system combines multiple high-tech layers—from XR and AI to orchestration and trust infrastructure. Ensuring seamless, interoperable deployment across diverse educational environments requires rigorous testing and integrator expertise.
- **Limited Sector-Specific Training Data.** AI-driven personalization and intent classification models rely on domain-specific datasets. The scarcity of real-world educational XR data—especially in 6G contexts—limits model performance and raises challenges in generalizability.
- **Digital Divide and Accessibility.** Despite improvements in XR affordability, many institutions (especially in underserved or rural areas) lack the digital literacy, infrastructure, or financial capacity to adopt immersive technologies, risking increased educational inequality.
- **Institutional and Regulatory Inertia.** Educational systems often operate under slow procurement cycles and cautious data governance practices. Despite technical readiness, institutional adoption may be delayed due to privacy sensitivities or uncertainty around new pedagogical models.

Opportunities

- **Post-Pandemic Hybrid Education Momentum.** The global shift toward hybrid learning has accelerated demand for persistent virtual classrooms. SAFE-6G directly addresses challenges exposed during the pandemic—engagement, security and adaptability—positioning itself as a transformative response.

- **Expansion into Vocational and Corporate Training.** SAFE-6G’s immersive and secure infrastructure is highly relevant for domains such as healthcare, engineering and safety training. These high-value sectors extend the market potential beyond formal education into lifelong learning and professional development.
- **Rising Demand for Ethical and Transparent AI.** Governments and educational authorities are increasingly requiring transparent, auditable and human-aligned AI in digital tools. SAFE-6G’s XAI assistant and privacy-respecting architecture provide a strong competitive edge aligned with this trend.
- **Access to Strategic Public Funding.** Programs like **Horizon Europe, Digital Europe** and national digital education initiatives actively support immersive learning, secure AI and inclusive digital transformation. SAFE-6G is well positioned to leverage such funding for scaling and standardization.
- **Technology Convergence (6G, XR, Edge AI).** The confluence of XR, edge computing and ultra-low latency 6G networks is unlocking previously unattainable educational scenarios. SAFE-6G is architected for this environment, enabling distributed, real-time immersive learning at scale.

Threats

- **Market Saturation and Proprietary Ecosystems.** Major tech players (e.g., Meta, Microsoft, Google) are building proprietary XR learning platforms tightly integrated with their ecosystems. Without strong partnerships or standardization backing, open frameworks like SAFE-6G may struggle for visibility and compatibility.
- **Privacy and Data Ethics Concerns.** Even with compliance measures, immersive educational platforms raise ethical concerns regarding behavioral tracking, profiling and biometric data use. Miststeps could erode institutional trust or attract negative public scrutiny—especially in K-12 settings.
- **Talent and Skills Gaps.** Successful operation of AI-driven XR systems requires expertise in networking, machine learning, immersive UI design and pedagogy. Many institutions lack such skills in-house, necessitating robust training and integration support services from SAFE-6G partners.
- **Regulatory Fragmentation Across Jurisdictions.** Privacy, AI explainability and identity management laws differ widely across regions. SAFE-6G must navigate these discrepancies to ensure full compliance, which may add cost and deployment complexity.
- **Hardware Fragmentation and Ergonomic Barriers.** Variability in XR device specifications, OS compatibility and user ergonomics introduces challenges in maintaining consistent experiences. Poor hardware comfort or inconsistent interaction quality, particularly for young learners, could hinder sustained adoption.

This SWOT analysis underscores SAFE-6G’s strategic readiness to disrupt the education sector through trust-aligned, immersive, and adaptive technologies. While challenges around integration, access and regulation exist, the platform’s **architectural flexibility, pedagogical relevance** and **alignment with emerging funding and policy priorities** position it as a high-impact innovation in the future of learning.

3.5.2.6 PORTER’S FIVE FORCES FRAMEWORK

Porter’s Five Forces framework provides a strategic lens to evaluate the competitive landscape and market forces shaping the adoption and scalability of SAFE-6G’s educational metaverse. While the metaverse for education is an emerging space, its convergence with AI, XR and next-generation

networking exposes it to various competitive pressures. Understanding these dynamics is essential for positioning SAFE-6G solutions effectively.

To assess the competitive dynamics surrounding the SAFE-6G educational metaverse, Porter’s Five Forces framework provides a strategic lens through which to evaluate both opportunities and pressures in the immersive EdTech ecosystem. The convergence of XR, AI and 6G infrastructure introduces unique complexities and SAFE-6G’s differentiated, trust-centric model must navigate these dynamics effectively to secure adoption and scale.

1. Threat of New Entrants – Risk: Moderate to High

While the EdTech sector has relatively low barriers for entry—particularly in software development—SAFE-6G’s deep integration of networked trust, AI orchestration and SSI makes replication difficult. Nevertheless, the growing availability of open-source development tools and public funding for digital education enables fast prototyping by startups and mid-size firms.

Factors reducing barriers to entry:

- Affordable XR hardware and public XR libraries.
- Open-source development platforms (e.g., Unity, Unreal Engine, TensorFlow).
- Policy incentives promoting digital transformation in education.

Factors increasing barriers to entry:

- Need for real-time, low-latency, 6G-ready infrastructure.
- Integration of privacy-by-design and trust enforcement mechanisms.
- Compliance with strict educational data regulations (e.g., GDPR, FERPA).
- Multi-layer orchestration across edge-cloud-network environments.

SAFE-6G’s edge: A trust-by-design architecture with dynamic orchestration, explainable AI, and verifiable credentials—elements beyond the current scope of most EdTech newcomers.

2. Bargaining Power of Suppliers – Risk: Moderate

The SAFE-6G stack relies on a broad range of **hardware and software providers**, including XR headset manufacturers, connectivity vendors and cloud orchestration platforms. While suppliers like Meta or HTC wield some power in the XR space, SAFE-6G’s **modular, standards-based architecture** mitigates vendor lock-in.

Factors lowering supplier power:

- Use of software-defined components and abstraction layers (e.g., Meta-OS, OpenCAPIF).
- Support for multivendor XR kits (e.g., IMM’s CloudXR compatibility).
- Open APIs and integration flexibility across trust, AI and orchestration layers.

Factors increasing supplier power:

- Limited availability of high-performance, affordable XR devices.
- Proprietary hardware ecosystems with restricted interoperability.
- Reliance on hyperscaler cloud infrastructure for scalability.

SAFE-6G's strategy: Leverage redundancy and openness in architectural design to ensure resilience and supply chain flexibility.

3. Bargaining Power of Buyers – Risk: High

Educational institutions, ministries, and corporate training providers are typically **few in number but large in influence**, demanding high customization, impact proof and long-term support. SAFE-6G must address these needs while differentiating from mainstream platforms.

Factors increasing buyer power:

- High switching costs and strong vendor preferences.
- Familiarity with incumbent platforms (e.g., Moodle, Microsoft Teams).
- Sensitivity to cost, regulatory compliance and IT integration effort.

SAFE-6G's mitigation tactics:

- Modular and phased adoption strategy with minimal disruption to existing systems.
- Deep integration options with LMS platforms and IT infrastructure.
- Strong focus on privacy, ethical AI and data sovereignty—key concerns for public education sectors.

SAFE-6G must balance technical performance with compelling value propositions, consulting support and demonstrable educational outcomes.

4. Threat of Substitutes – Risk: Moderate

While SAFE-6G introduces a novel immersive learning model, **partial substitutes** exist—such as video conferencing (Zoom), LMS platforms (Canvas) and low-end XR content providers (ClassVR). These options are simpler and more familiar, especially for cost-sensitive institutions.

Substitution risk drivers:

- Prevalence of video-based hybrid learning models post-pandemic.
- Budgetary limitations in public education.
- Low complexity and faster deployment of traditional LMS and conferencing tools.

SAFE-6G's differentiation:

- Persistent, AI-enhanced metaverse classroom with spatial presence and trust orchestration.
- Real-time feedback and personalization via explainable AI and cognitive coordination.
- Adaptive security and privacy enforcement during learning sessions.

Strategy: Focus on demonstrating improved engagement, inclusivity, learning outcomes and long-term return on investment (ROI).

5. Industry Rivalry – Risk: High

The immersive learning market is highly dynamic and **rapidly evolving**, with major tech players and consortia investing heavily in education-oriented XR and AI platforms. The space is characterized by aggressive innovation cycles and competing standards.

Rivalry intensifiers:

- Significant private and public investment in immersive EdTech post-COVID.
- Major tech ecosystems pushing proprietary XR education platforms (e.g., Microsoft Mesh, Meta Quest for Education).
- Overlap with training, entertainment, and remote collaboration platforms.

SAFE-6G's unique position:

- Integrated 6G network functions with cognitive orchestration and explainable trust mechanisms.
- Modular, standards-compliant architecture adaptable to a range of educational scenarios.
- Commitment to open access, inclusivity, and ethical digital transformation.

SAFE-6G should continue fostering alliances with ministries, universities, standardization bodies and EdTech vendors to ensure scalability, interoperability, and market credibility.

The SAFE-6G educational metaverse faces a competitive yet opportunity-rich environment. By emphasizing trust, personalization, modularity, and interoperability, it can position itself as a future-proof, ethical and impactful solution in the global shift toward immersive digital education.

3.5.2.7 LLAVA MATRIX ANALYSIS

The **Llava Matrix** provides a multidimensional framework to assess how the components of **SAFE-6G Use Case 2** collectively deliver on functional, strategic, and trust-centric goals in immersive education. Unlike linear planning models, the Llava Matrix emphasizes system co-evolution, dynamic orchestration, and continuous adaptation—qualities that are essential for a resilient and scalable hybrid learning metaverse.

User Needs and Operational Context

SAFE-6G targets a wide range of users across the educational ecosystem, each with unique operational demands:

- **Instructors** require tools to communicate complex concepts across physical and digital spaces while ensuring content integrity and student engagement.

- **Learners** seek intuitive, emotionally engaging and personalized learning environments that transcend passive video-based interactions.
- **Administrators** demand systems that are secure, privacy-compliant and compatible with existing IT infrastructure, while being adaptable to policy and governance needs.

SAFE-6G addresses these needs through:

- Conversational AI and intent classifiers for natural, adaptive interaction.
- Immersive XR experiences using CloudXR kits to enhance spatial awareness and collaboration.
- Real-time trust orchestration to personalize privacy, safety and access policies.
- Edge-cloud orchestration for resilient, responsive system performance under variable loads.

Technology–Capability Alignment

<i>Capability Required</i>	<i>Technological Enabler(s)</i>	<i>Integration Role</i>
Real-Time Hybrid Collaboration	CUMUCORE (5G/6G Core), IMM (CloudXR Kit), UPV (Meta-OS)	Supports low-latency, high-bandwidth XR interaction across co-located and remote users.
Adaptive Learning Support	NCSR (Chatbot, Cognitive Coordinator), Eviden (MLOps)	Enables AI-driven personalization of learning pathways based on intent and behaviour.
Explainable Feedback and Transparency	THALES (XAI Assistant), INF (Intent Chatbot App)	Provides transparent AI decisions, improving user confidence and ethical compliance.
Policy-Driven Access and Privacy Control	SPACE (Privacy Function), Eviden & InQbit (SSI), eBOS (SDP Function)	Ensures secure, personalized access and protects learner data in real time.
Secure API Interoperability	Telefónica (OpenCAPIF)	Facilitates standardized, secure integration with third-party educational tools.
Seamless Deployment and Resource Mgmt.	UPV (Meta-OS), UNIWA (Resilience Function)	Allocates resources dynamically across edge/cloud layers for optimal performance.

Table 20: SAFE-6G Technology–Capability Alignment

Strategic Value Streams

The Llava Matrix also highlights the broader institutional and societal value SAFE-6G enables:

- **Trustworthy Digital Pedagogy:** Ethical, explainable AI tools align with educational values of fairness, inclusivity and transparency—building trust among students, educators and regulators.
- **Scalable Hybrid Education:** Modular kits and dynamic orchestration enable gradual scaling—supporting pilots in small departments and full-scale rollouts at national levels.
- **Inclusive Accessibility:** By supporting diverse devices and connectivity levels, SAFE-6G lowers digital barriers for under-resourced or geographically dispersed institutions.

- **Responsive Learning Environments:** Real-time adaptation through the Cognitive Coordinator ensures the learning space evolves with user behaviour, system performance and context.
- **Institutional Autonomy:** Decentralized SSI, on-premises XR deployment and customizable trust policies ensure alignment with legal and organizational governance models.

Emerging Gaps and Future Refinements

While the architecture is forward-looking, several areas require additional development to ensure robustness and adoption readiness:

- **Legacy System Interoperability:** Many institutions still depend on legacy LMS and IT systems. Middleware and API wrappers are needed for seamless integration of SAFE-6G modules.
- **Contextual AI Training Data:** A lack of domain-specific datasets limits the accuracy and adaptability of AI models. SAFE-6G should prioritize the ethical collection and anonymization of interaction data in real classrooms.
- **Trust Function Arbitration:** Overlapping triggers from privacy, resilience and identity systems may require refinement of the coordination logic via policy engines or arbitration layers.
- **XR Ergonomics and Accessibility:** Ensuring comfort, safety and usability for all learners—including those with disabilities or sensory sensitivities—requires continuous UI/UX improvement and compliance with safety standards.
- **Standardization Readiness:** As educational XR and AI standards continue to evolve, SAFE-6G must align key components (e.g., OpenCAPIF, SSI) with emerging ETSI, IEEE and ISO guidelines to secure future interoperability and regulatory approval.

The Llava Matrix illustrates how SAFE-6G Use Case 2 operates as a cohesive ecosystem of trust, AI and immersive technologies that respond intelligently to educational needs. It reveals both current capabilities and the roadmap for strategic evolution, supporting a future of inclusive, ethical, and high-impact digital learning at scale.

3.6 CONCLUSION & NEXT STEPS

The exploitation and IPR management framework developed in SAFE-6G is structured to reflect the complex, multi-stakeholder nature of the project. It is built upon a **dual-level model** that combines:

- **Individual Exploitation Plans**, which articulate each partner’s pathway for leveraging their results based on their technological contributions, business models and strategic objectives, and
- A **Joint Exploitation Strategy**, designed to coordinate and amplify the collective value of project results, aligning technical synergies with market opportunities and societal needs.

Together, these layers ensure that the full spectrum of SAFE-6G’s innovation outcomes—ranging from XR-enabled metaverse solutions and AI orchestration to privacy and trust infrastructures—are positioned for uptake in diverse application domains.

Key Outcomes to Date

- Each partner has defined background and foreground IP, aligned with the CA and GA and clarified how their results will be used post-project—whether through commercialization, licensing, research continuity, or integration into existing portfolios.
- The joint exploitation strategy has applied multiple business assessment tools—Lean Business Canvas, SWOT analysis, Porter’s Five Forces and the Lava Matrix—to develop coordinated plans around shared use cases, such as the Industrial Metaverse and Metaverse for Education.
- A first wave of interoperable assets and demonstrators (e.g., the CloudXR Kit, trust orchestration modules, AI-driven chatbots) has been identified, with pathways for modular adoption by industry and public stakeholders.
- The consortium has established an IPR tracking approach that promotes transparency, identifies potential licensing models and facilitates open-access dissemination where appropriate.

Next Steps Toward Final Exploitation and IPR Deliverable (D6.6)

As the project progresses toward completion, several actions will be prioritized to refine, consolidate, and validate both individual and joint exploitation plans:

- **Review and Update of Individual Plans.** Each partner will revisit their exploitation roadmap based on technical progress, pilot feedback and updated market intelligence. This includes refining TRL assessments, go-to-market strategies, and target stakeholders for each key asset.
- **Consolidation of Joint Value Propositions.** The project will continue integrating individual components into cohesive solution packages and demonstrators. A special focus will be placed on documenting joint assets and identifying commercial or public-sector deployment opportunities.
- **Finalization of the IPR Framework.** Although no centralized enforcement body is foreseen, partners will validate and formalize final IPR usage conditions, licensing intentions and collaboration agreements. This will include any updates to IP declarations and terms for open-access resources.
- **Completion of Deliverable D6.6: Final Exploitation and IPR Management Plan.** Scheduled for the end of the project, D6.6 will serve as the comprehensive synthesis of all exploitation-related work.

In conclusion, the exploitation and IPR activities in SAFE-6G reflect a robust, partner-driven and impact-oriented approach. The framework ensures that all project outcomes, whether individually developed or co-created, are supported by clear rights, actionable plans and aligned incentives. As we move into the final project phase, emphasis will shift toward concrete deployment scenarios, partner commitments and sustainable pathways to ensure that SAFE-6G results are carried forward into real-world applications, policy influence and continued innovation.

4 CONCLUSION

This deliverable presents an update on the implementation of the strategies outlined in D6.2 for the SAFE-6G project's standardisation, innovation, exploitation, and technology transfer activities. It serves as a critical intermediate milestone, offering both a progress report and a foundation for the final outcomes to be presented in D6.6.

In terms of standardisation, the deliverable refines the initial categorisation of contributions into three main axes: (1) monitoring and information gathering, (2) active engagement and collaboration, and (3) contribution to and influence on standardisation processes. These refined categories ensure a targeted and scalable approach to influencing future 6G standards. As a result, SAFE-6G has established initial but strategically important connections with four major SDOs and initiatives: 3GPP (specifically SA1, SA3, and SA6), ETSI (OCP and SAI), CAMARA, and ENISA. These engagements align closely with SAFE-6G's core technical domains—trust, AI security, 6G API ecosystems, and overall trustworthiness and represent the early steps toward impactful contributions to the evolving 6G landscape.

On the innovation and exploitation sections, the deliverable details the individual exploitation plans developed by each partner. These plans articulate how each organization intends to leverage its contributions—ranging from open-source assets to commercial offerings—and define the expected market and technological impact. A curated list of KERs has been compiled from these plans, representing the project's most valuable and innovation-driven outcomes. Each KER has been rigorously evaluated using a multi-criteria scoring framework, incorporating dimensions such as technological maturity, commercial potential, strategic alignment, and scalability. This evaluation supports a structured understanding of the project's exploitation potential and helps prioritize follow-up actions.

Furthermore, the deliverable lays the groundwork for joint exploitation, with initial work completed on two representative use cases: the Industrial Metaverse of a Production Line and the Metaverse for Education. These use cases are being developed into coherent exploitation plans that integrate multiple project outcomes into high-impact, demonstrable applications, enabling effective technology transfer and market readiness.

Overall, Deliverable D6.4 demonstrates strong alignment between the technical work packages and the downstream exploitation and standardisation efforts. The progress reported here will be further expanded and consolidated in Deliverable *D6.6-Standardisation, Innovation, Exploitation and Technology Transfer Activities (Final)*, due at Month 36, which will present the final synthesis of SAFE-6G's contributions to standardisation bodies, the innovation ecosystem, and future 6G market adoption.

5 REFERENCES

- [1] [Online]. Available: <https://www.marketsandmarkets.com/Market-Reports/self-sovereign-identity-ssi-market-73711961.html#:~:text=Overview,90.5%25%20during%20the%20forecast%20period>
- [2] [Online]. Available: <https://www.marketresearchfuture.com/reports/self-sovereign-identity-market-22208>
- [3] [Online]. Available: <https://www.w3.org/TR/did-core/>
- [4] [Online]. Available: <https://www.nist.gov/publications/zero-trust-architecture>
- [5] [Online]. Available: [Machine Learning Operations Market Size | CAGR of 43.2%](#)
- [6] "A Multivocal Review of MLOps Practices, Challenges and Open Issues". Available: <https://arxiv.org/pdf/2406.09737v1>
- [7] [D2.2 SAFE-6G v1.0.pdf](#)
- [8] [Online]. Available: [7 Ways Businesses Can Benefit From Open-Source Software - Clearcode](#)
- [9] [Online]. Available: <https://www.fortunebusinessinsights.com/industry-reports/software-defined-parameter-market-100378>.
- [10] [Online]. Available: <https://www.transparencymarketresearch.com/software-defined-perimeter-market.html>.
- [11] [Online]. Available: <https://www.imarcgroup.com/cloud-continuum-market>