6GSNS

Co-funded by the European Union

SAFE-6G

SAFE-6G

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

Deliverable D2.1: Definition of Technical Requirements for User-centric 6G Trustworthiness

Date: 18/12/2025

Version: v1.1

DISCLAIMER

Grant Agreement	101139031
Document number	D2.1
Document title	Definition of Technical Requirements for user-centric 6G Trustworthiness
Lead Beneficiary	THA
Editor(s)	Stéphane Lorin, Alan Branchereau, Pascal Bisson (THA)
Author(s)	Harilaos Koumaras (NCSRD) Spyridon Georgoulas (NCSRD) Vicky Rentoula (NCSRD) Kushal Mehta (IQBT) Dimitris Uzunidis (UNIWA) Panos Karkazis (UNIWA) Daniel García Sanchez (TID) Álvaro Andrés Anaya Amariles (TID) Javier García Rodrigo (TID) Nikolaos Vryonis (INF) Konstantinos Fragkos (INF) Eugenia Vergi (INF) Vaios Koumaras (INF) Alejandro Fornes (UPV) Charles Bailly (IMM) Dimitris Zouzias (eBOS) Marios Sophocleous (eBOS) Stephane Lorin (THA) Alan Branchereau (THA) Pascal Bisson (THA) Apostolis Garos (SHG) Ricardo Marco (ATOS) Sonia Castro (ATOS) Guillaume Hébert (ATOS)
Dissemination level	Public
Contractual date of delivery	31/08/2024
Status	Final
File name	SAFE-6G_D2.1_V1.1.pdf

Revision History

Version	Description
V0.1	Work split per partner
V0.2	Table of Contents
V0.3	Initial Contributions by all involved partners
V0.4	Second round of contributions by all involved partners
V0.5	First revision and homogenisation of the content conducted by UPV and CMC
V0.6	Additional input in the definition of trust and trustworthiness
V0.7	Additional input in the cognitive coordinator and XAI of SAFE-6G ecosystem
V0.8	Additional input on user-centric, USN/NSN, Trust functions, second revision
V0.9	Internal review and homogenisation of the content
V1.0	Release of D2.1 following the Quality Check
V1.1	Updated version after mid-term review

GLOSSARY

Abbreviations/Acronym	Description
AI	Artificial Intelligence
AMF	Access Management Function
API	Application Programming Interface
AR	Augmented Reality
B5G	Beyond 5G
cLoT	calibrated Level of Trustworthiness
DID	Decentralized Identifiers
DLT	Distributed Ledger Infrastructure
DP	Differential Privacy
DT	Digital Twin
EC	European Commission
FL	Federated Learning
GDPR	General Data Protection Regulation
HA	High Availability
IAP	ICT application provider
InfP	Infrastructure Provider
LoT	Level of Trustworthiness
ML	Machine Learning
MNO	Mobile Network Operator
N/A	Not available
NF	Network Function
nLoT	non-calibrated Level of Trustworthiness
NLP	Natural Language Processing
NLU	Natural Language Understanding
NRF	Network Repository Function
NSN	Network Service Node
OSC	Open Source Community
PS	Privacy Score
QoE	Quality of Experience
QoS	Quality of Service
RBO	Regulatory Body Organisation
REST	Representational State Transfer
RTO	Research and Technology Organisation
SBA	Service Based Architecture
SDO	Standard Developing Organisation
SDP	Software Defined Perimeter
SFC	Service Function Chaining
SSI	Self-Sovereign Identity
SSP	Security Service Provider
TS	Tier-1 Supplier
TV	Telecom Vendor
UPF	User Plane Function
USN	User Service Node
VC	Verifiable Credential
VR	Virtual Reality

XAI	eXplainable AI
XR	Extended Reality

EXECUTIVE SUMMARY

The 6G vision for an open, distributed and user-centric evolution of the current Service Based Architecture (SBA) core network creates many security challenges and risks. In the envisioned 6G ecosystem, trusted connections are critical for all parties involved, extending security and privacy to a more inclusive framework, such as trustworthiness, which should be assured as a native feature. The most significant paradigm adjustments in the envisioned user-centric 6G system are the shift from a security-only focus to a broader scope of native trustworthiness, clarifying that the term "trustworthiness" refers to a holistic approach, including safety, security, privacy, resilience, and reliability. SAFE-6G aims at implementing such a trustworthy framework to support and enhance the trust over the next evolution of the 5G network and the managed resources.

This document introduces a reference architectural blueprint to instantiate this new trustworthy 6G ecosystem. The impact of this new paradigm is also analysed from the point of view of the different stakeholders and actors linked to 5G/6G networks and the new roles, consents and opportunities it implies for them.

Based on the architectural blueprint, different domains have been defined grouping together building blocks and components that have been identified. For each domain, an extended set of functional and non-functional requirements has been proposed towards realising this blueprint to a detailed architecture in D2.2 that will drive the proof-of-concept implementation and validation of the SAFE-6G ecosystem in WP5. These requirements create a highly ambitious view of the envisioned 6G framework and provide strong guarantees, to related stakeholders, about the impact and ambition that can be achieved by the project.

Lastly, ambitious Use Case scenarios are presented along with some initial specific requirements.

This document is the first deliverable of *WP2- Realisation Process, Requirements and Reference Architecture Design* and will be completed in the next months by two other deliverables: *D2.2- Overall SAFE-6G Framework and Reference Architecture Design* (due in M10/October 2024) and *D2.3- Metaverse use-cases definition with virtual-assistant for user-centric configuration* (due in M12/December 2024).

KEYWORDS

6G, Trustworthiness, System Requirements, Stakeholder, Use case

TABLE OF CONTENTS

List of FIGURES

1 INTRODUCTION

1.1 OBJECTIVE OF THE DOCUMENT

The SAFE-6G project aims at providing an end-to-end cognitive trustworthiness framework for user-centric distributed 6G networks over the edge-cloud continuum. To achieve this goal, the consortium members are developing a reference blueprint architecture, involving multiple building blocks and components interacting with each other. To ensure that these components can provide the expected features and services, and to assess the compliance of the system to the user's expectations, key Technical Requirements must be defined. This deliverable describes and lists those technical requirements that will guide the definition of the SAFE-6G architecture, as well as the development of the SAFE-6G prototype ecosystem.

1.2 STRUCTURE OF THE DOCUMENT

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

- Chapter 2 introduces a version of the SAFE-6G framework vision, providing some context on 6G trustworthiness that is useful for the reader to better understand the SAFE-6G motivation, which leads us to the SAFE-6G architectural blueprint (it will be later formalized in D2.2) and the definition of the relevant stakeholders and system requirements.
- Chapter 3 introduces an overview of the use cases that will be developed in the project. The detailed use-case-related requirements will be integrated in deliverable D2.3.
- Chapter 4 depicts the methodology followed to define the SAFE-6G requirements, along with a set of instructions that guided their gathering.
- Chapter 5 presents the list of all the SAFE-6G requirements regarding the different concerned domains.
- Conclusion And Next Steps presents a summary of the work done and the next steps.

1.3 TARGET AUDIENCE

At consortium level, the primary audience for this deliverable comprises the partners involved in the technical part of SAFE-6G project and the end users who will use and validate the SAFE-6G ecosystem. Since this deliverable is public, the content of this deliverable such as the definition of the 6G Trustworthiness at user-centric level, the design blueprint, as well as all the requirements that are defined in this deliverable will contribute to the adoption of SAFE-6G approach for building a trustworthy and user-centric 6G system.

2 SAFE-6G Motivation and Design Principles

The 6G vision for an open, distributed and user-centric evolution of the current Service Based Architecture (SBA) core network creates many security challenges and risks. The disaggregated heterogeneous cloud continuum (i.e., distributed cloud system with many stakeholders located in different regions, while private, public, or hybrid clouds are considered for the formation of the continuum), in conjunction with softwarization and IT-based infrastructure operations, sets the stage for risks and challenges to trustworthiness in the 6G era.

The existing 5G security architecture is adaptable to a centralized network architecture, and in 5G, trust connections between network parts are created at the protocol level, rather than involving device and network behaviour. In the envisioned 6G ecosystem, trusted connections are critical for all parties involved, extending security and privacy to a more inclusive framework, such as trustworthiness, which should be assured as a native feature.

Therefore, the most significant paradigm adjustments in the envisioned user-centric 6G system are the shift from a security-only focus to a broader scope of native trustworthiness, clarifying that the term "trustworthiness" refers to a holistic approach, including safety, security, privacy, resilience and reliability.

2.1 Trustworthiness and Level of Trust Relation

Currently, IMT 2030 promotes trustworthiness as a new attribute for the 6G vision. In fact, numerous standard groups [1] , including 3GPP, ETSI, and IEEE, have been working on trustworthiness issues. Meanwhile, the world's main communications suppliers have explicitly underlined the importance of 6G trustworthiness in their 6G projects, proposals, and white papers. In addition, several scholars have produced technical papers on the definition, generation, protection, and optimization of trustworthiness. All of these suggests that trustworthiness will become an essential characteristic in 6G, but still, it remains confusing the use of trustworthiness and trust terms.

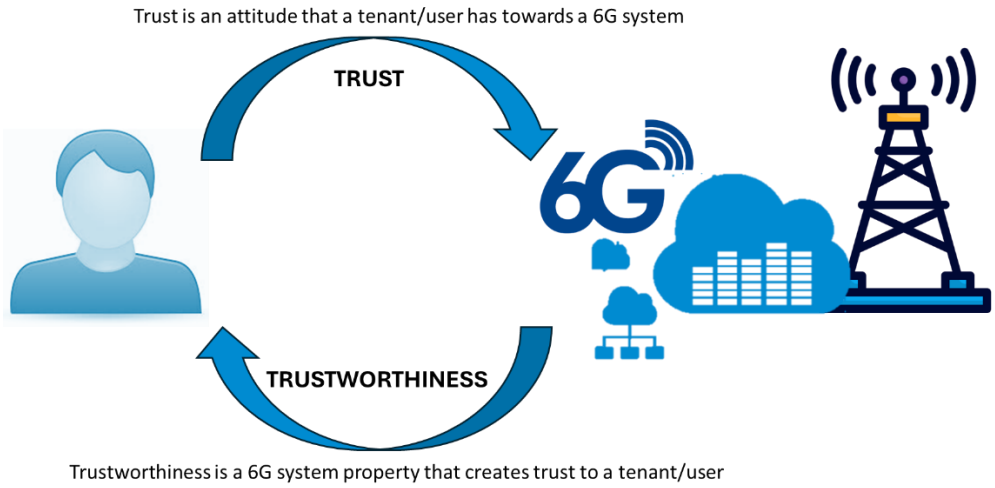


Figure 1: 6G system Trustworthiness and tenant/user trust relationship

Despite the discrete meaning and scope of trustworthiness, it is still observed its misuse as trust. For this reason, the SAFE-6G Consortium strongly believes that it is necessary to start by defining the meaning and relation of trustworthiness and trust, which will be repeatedly used in the SAFE-6G documentation, so it is of highest importance their meaning to be clear and sound.

Trust is an attitude that a tenant has towards a 6G system. In contrast, trustworthiness is a system property that creates trust to the 6G tenant/user. Thus, a user/tenant trusts (or requires a specific level of trust from) a 6G system, because the 6G system is trustworthy. In other words, the trustworthiness of a 6G system contributes to building the trust level of the tenant/user of the specific system. Thus, the more trustworthy the 6G system is, the higher the trust level of the tenant/user will be [2] .

2.2 User-centric and AI-Assisted Coordination of 6G System Trustworthiness

The most significant paradigm adjustments in the envisioned user-centric 6G system are the shift from a security-only focus to a broader scope of native trustworthiness, clarifying that the term "trustworthiness" refers to a holistic approach, including safety, security, privacy, resilience and reliability as trustworthiness dimensions and properties. 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 dimensions/properties by dealing with a security-by-design approach, as well as a wide range of themes, such as the trust model, which will be examined in WP4, and the application of a novel cognitive coordination component (e.g., Intent-based trustworthiness, based on Artificial Intelligence (AI) / Machine Learning (ML) techniques).

Considering that each tenant/user has different requirements in terms of trust level from a 6G system, it is created the need the 6G system to be capable of being adapted to the specific needs (i.e., trustworthiness level) that corresponds to the level of trust and requirements of each specific tenant/user. Therefore, the 6G system should not be only trustworthy in a static way, but it should become user-centric and capable of dynamically adapting the trustworthiness level to the trust level requirements of each tenant. The user-centric approach in 6G system allows for dedicated network services to be provided at the granularity of the user by configuring appropriately the 6G system (i.e., the core network functions) [3] .

In order to achieve this user-centric and intent-based driven trustworthiness dynamic configuration of a 6G system, it is necessary to be introduced in the SAFE-6G concept a AI/ML-assisted coordination component, which will act as an intent-handling function that comprehends sophisticated and abstract trust intent semantics (divided into the five trustworthiness dimensions/taxonomies of Safety, Security, Privacy, Resilience, and Reliability), and calculates the ideal goal state and organizes activities to transition the SAFE-6G system into this trustworthy state.

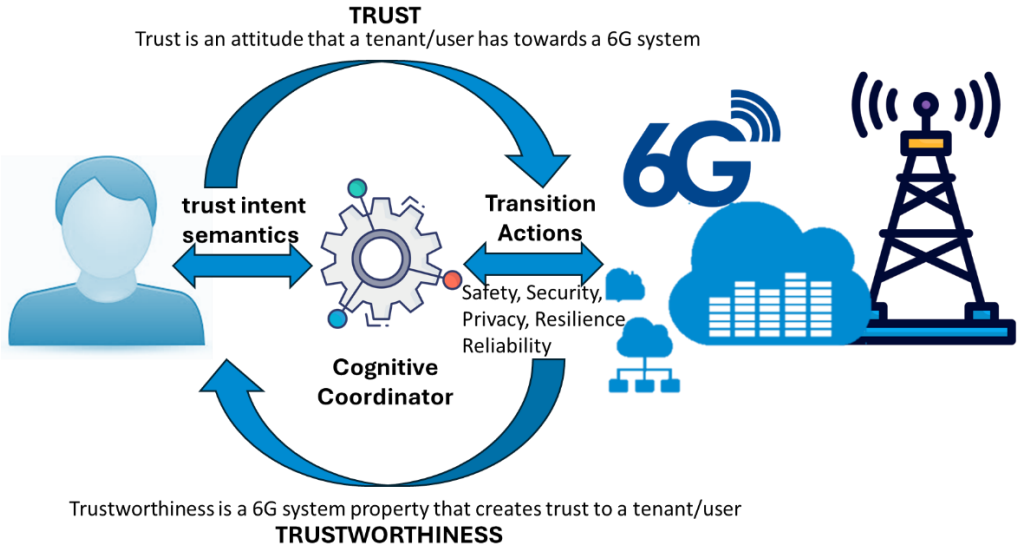


Figure 2: User-centric and AI-assisted coordination of 6G trustworthiness

The AI-assisted coordinator should perform the process of mapping the trust-intent semantics received by the tenant/user into transition actions of the 6G system via configurations in the trustworthy dimensions of the 6G system, (i.e., into the safety, security, privacy, resilience, and reliability domains). Given that this autonomous mapping is a technical application of cognition (since it is designed to perform the operational tasks of understanding by experiencing and monitoring), the envisioned AI-assisted coordinator is named Cognitive Coordinator.

2.3 The Complementary Role of XAI at Optimizing the Level of Trust

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, based on AI/ML techniques).

This impact of trustworthiness measures on the usability of the system by the tenant may impact the perceived level of trust if the user is not fully understanding the reason that the system takes the actions that are affecting them. Explainability is often viewed as an effective way to build trust among stakeholders. If users have a better understanding of the process by which the system generates its outputs and the explanation provided for a particular result aligns with their preconceptions of what constitutes a proper decision, then the level of trust of the system has been improved. The literature does, in fact, frequently link explainability to trust [4] ,[5] , and many researchers—at least tacitly—assume that explainability and trust are strongly related [6] ,[7] . This relationship is known as the Explainability-Trust-Hypothesis, which states that "*Explainability is a suitable means for facilitating trust in a stakeholder*."[2]

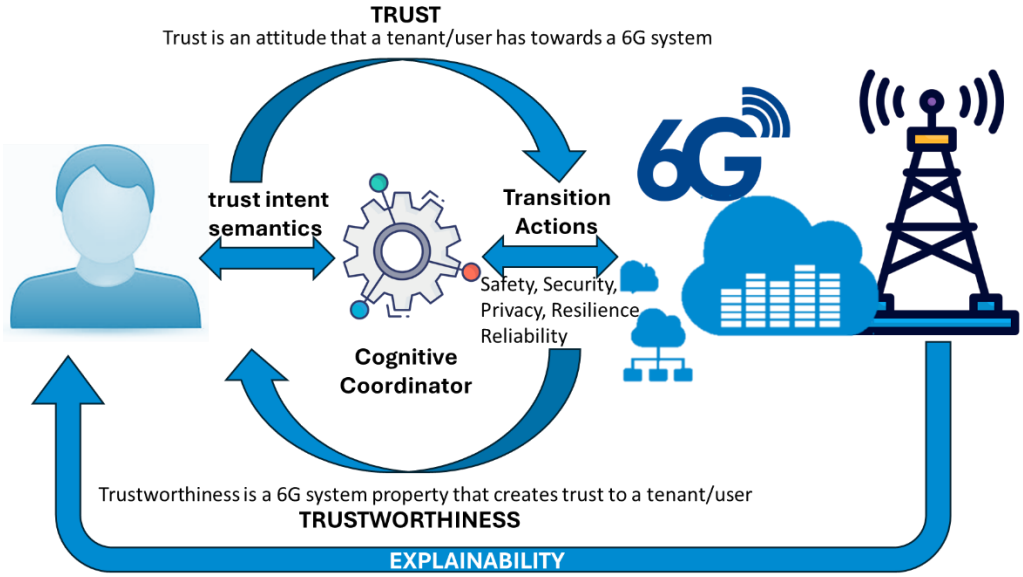


Figure 3: Explainability as an additional means for improving the Level of Trust in SAFE-6G

Among the various explainability tools, SAFE-6G as a modern system has selected in its design principles the use of eXplainable AI (XAI) [8] to complement the operation of the Cognitive Coordinator and contribute to the improvement of the tenant's/user's Level of Trust over the Trustworthy 6G System. As evidenced by the "right to explanation" outlined in the General Data Protection Regulation (GDPR) and the European Commission's (EC) Technical Study on "Ethics recommendations for trustworthy AI" [9] , trustworthiness has become crucial for both users and governmental organizations. They claim that explainability is a crucial element of trustworthiness. As a result, XAI, or an AI "that creates information or reasoning to make its working obvious or easy to understand," is receiving more and more interest from both industry and academia. In this context, two strategies for achieving explainability can be identified: The adoption of post-hoc explainability techniques (i.e., the "explaining black-box" strategy) and the design of inherently interpretable models (i.e., "transparent box design" strategy). These approaches allow to understand the model behaviour and can be integrated in the model training or being applied as post-hoc approaches, after ML training. SAFE-6G will focus on the first method, because it allows to add the interpretability layer without changing the model training – which is performed within the MLOps lifecycle, using Global XAI methods and Local XAI methods, which will be further analysed in WP4.

2.4 User-Centric Networking

The transition from 5G to 6G represents a pivotal moment in the evolution of telecommunications, signifying a leap towards a more user-centric network. This shift is revolutionary, as it promises to redefine the interaction between users and network services. This innovative approach is distinguished by several key features, such as personalized network instances and automated, intelligent, and dynamic optimization of resource management. These contribute to the creation of a networking environment that is more personalized, efficient, and secure. The network is now more tailored to each separate user/group of users' needs and allows them to control their personal data and policies, thereby ensuring each user's quality of experience (QoE) level. This is achieved through

the integration of advanced and intelligent optimization mechanisms and technologies that continuously analyze user behavior and preferences, thereby facilitating a more intuitive and responsive network.

In 6G networks, user-centric networking represents a fundamental shift from traditional network architectures, recentring the focus on individual users rather than on network functions alone. This approach envisions a highly flexible, adaptive network structure where users are empowered to define, configure, and control their network experiences. Unlike the static, monolithic frameworks of previous generations, 6G aims to provide a modular, decentralized network setup. This allows users not only to manage their own digital assets and data ownership but also to actively participate in the creation and management of network services and applications.

In [10] the author proposes a framework for a core network, describes the network and user nodes, and suggests the use of a DLT platform for the secure and trustworthy control of data. The user node includes a reduction in the number of message exchanges among functions and an improvement in network efficiency. The decentralized architecture and reliable data management allow users to control their digital assets. The user domain could be extended to any range of resources in the user node of a mobile communication system. Further refinement of the user-centric network (UCN) implementation is required, including the elaboration of the user node lifecycle and the provision of concrete examples of the specific interaction processes between the network and user nodes.

UCN Definition in [10] : The user-centric approach to network architecture offers a personalized and flexible system compared to the traditional network-centric model. It allows users to define, configure, and control their network services, leading to a more interactive relationship between users, services, and applications. This approach not only reduces signaling and latency by maintaining user-specific states but also simplifies communication protocols, making the system more cost-effective and easier to manage. Additionally, it aligns well with decentralized technologies, enhancing security against common threats like SPoF and DDoS attacks.

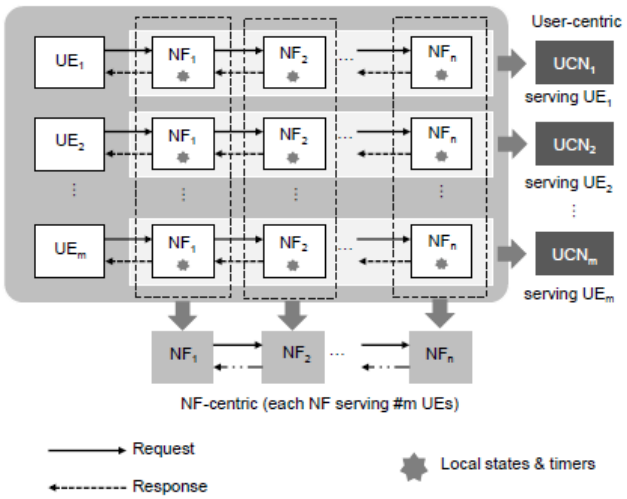


Figure 4: Comparison of concepts between user-centric and network-centric approaches, e.g. in the core network.

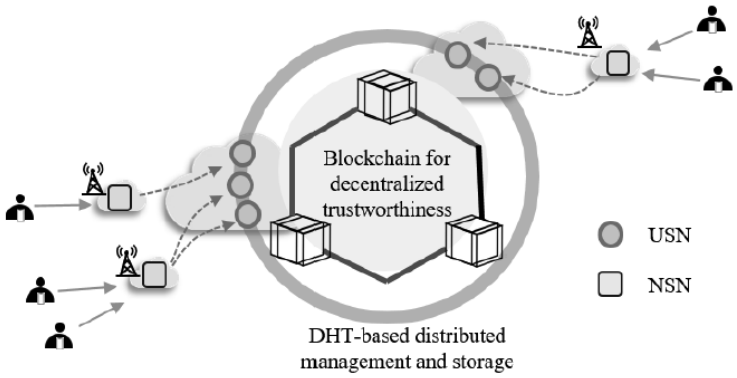


Figure 5: The novel UCN architecture is composed of USNs, which are deployed as DHT nodes and implement all the necessary functionalities for mobile users to access services.

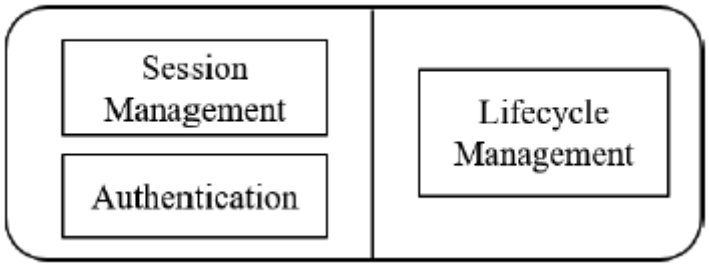


Figure 6: The functional structure of NSN is equipped with select lightweight functions of core networks and is responsible for the lifecycle management of USN.

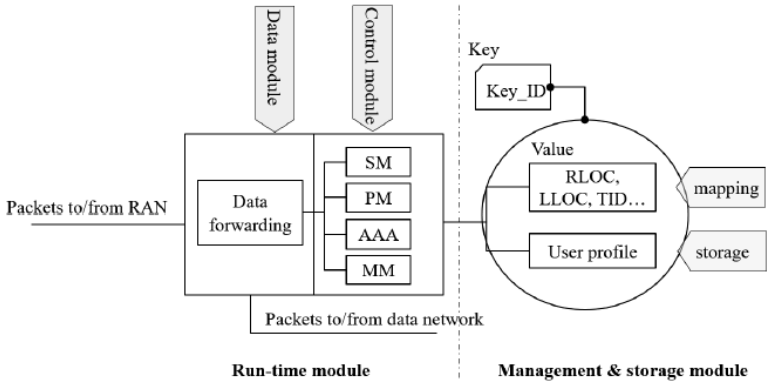


Figure 7: The functional structure of the USN comprises two principal modules: the run-time module, which is responsible for the execution of functions within the core networks, and the management and storage module, which is primarily utilized for data operation.

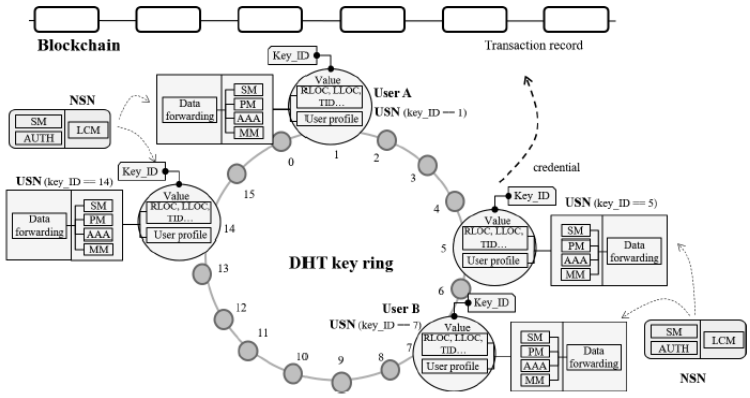


Figure 8: Illustration on the UCN implementation.

In [11] the authors present an analysis of a user-centric approach to network design, which entails the creation of an ultra-dense network. The implementation of 3D user distribution in large-scale building units has been demonstrated to enhance the overall volume of user flow. The implementation of UCN facilitates enhanced user experience, as it optimizes its quality, the range of available services, and the underlying infrastructure.

UCN Definition in[11] : In a user-centric network the serving access point (AP) is being adaptive to satisfy the user equipment (UE). An ultra-dense network has more APs than UEs. This network sensing allocates resources and provides seamless services in UEs. It introduces four key entities split between the Radio Access Network (RAN) and Core Network (CN) sides, which separate user and control planes to enhance data management and user policy control. As the 6G era approaches, the application and practicality of UCN will undergo a critical reassessment to support increasingly dense networks, utilize high-frequency resources, and enable new services.

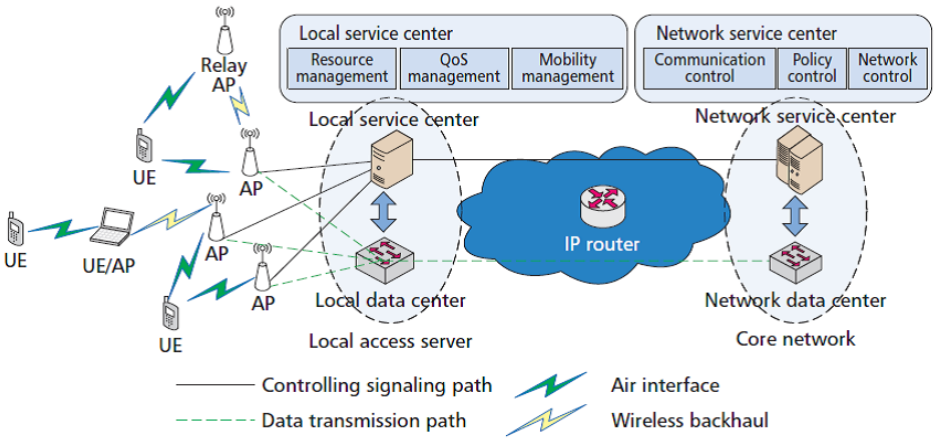


Figure 9: Network architecture of user-centric ultra-dense network.

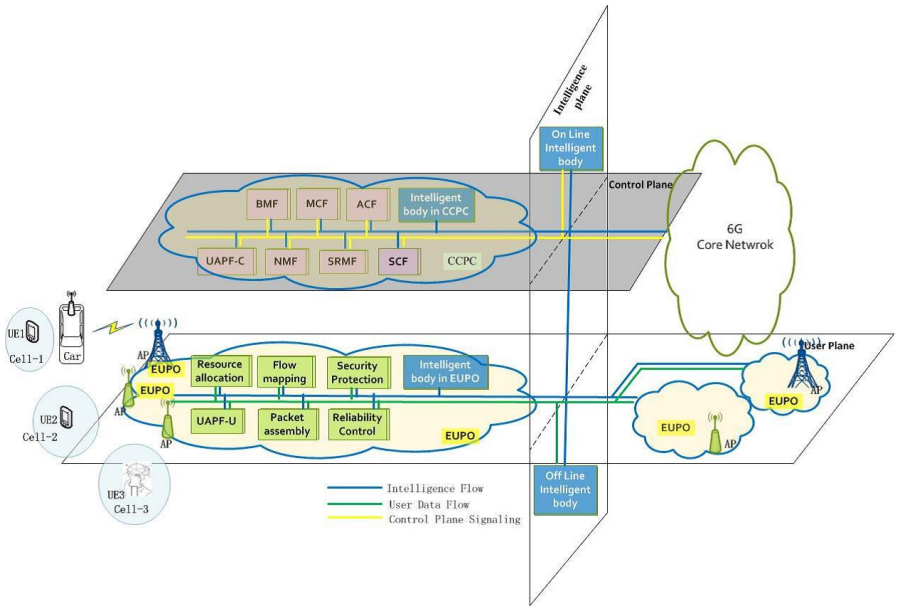


Figure 10: The architecture of AI-native user-centric network for 6G.

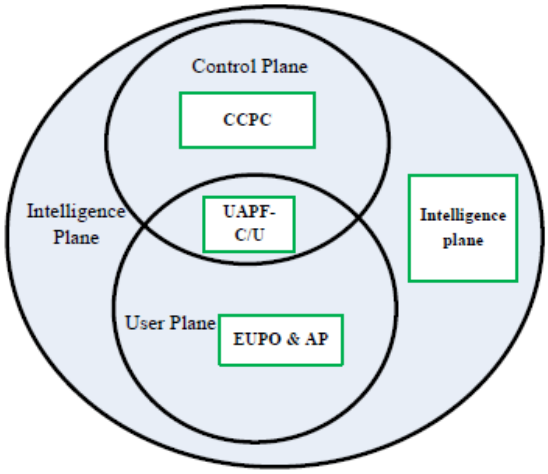


Figure 11: The relationship of the key technologies.

In [12] , the authors present an analysis of the advantages of a user-centric approach to the RAN. The network comprises multiple nodes, which collectively offer a high data rate and consistent user experience. Furthermore, the cell range is automatically adjusted in accordance with the prevailing circumstances. It would be beneficial to develop a secure, scalable, and unified method for managing multiple users in a given area.

UCN Definition in [12] *:* The User-Centric Access Network (UCAN) for 6G is designed to deliver high-speed, consistent services tailored to individual users within a local coverage area. It aims to address the varied demands of future 6G environments by providing a scalable and adaptable framework. UCAN operates as a de-cellularized network, offering a universal structure that allows for the flexible management of different APs across multiple platforms. This ensures the provision of on-demand

services to users. The network's serving area, termed a 'flexible cell', is customized in real-time for each user, adapting to their movement, service needs, and available APs, without being constrained by physical boundaries.

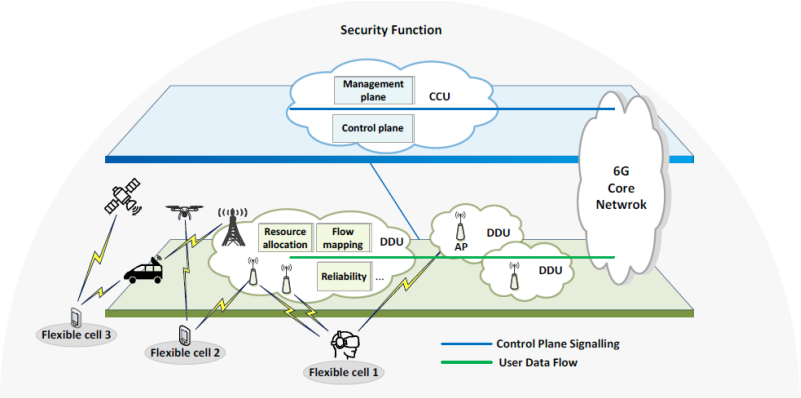


Figure 12: The basic architecture of user-centric access network.

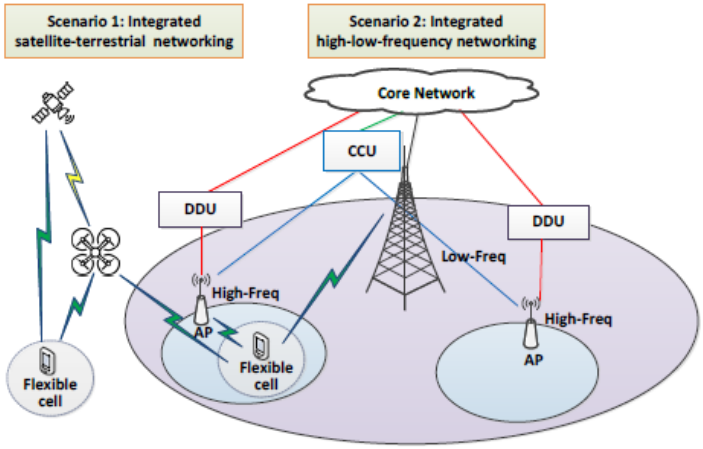


Figure 13: Two typical networking technologies.

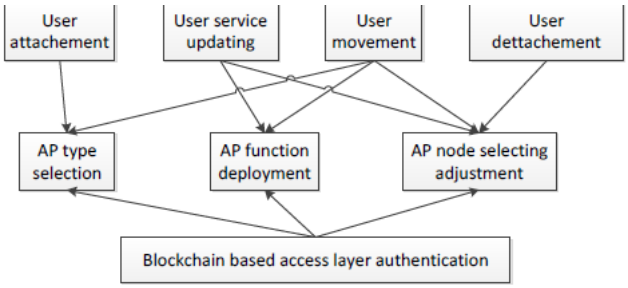
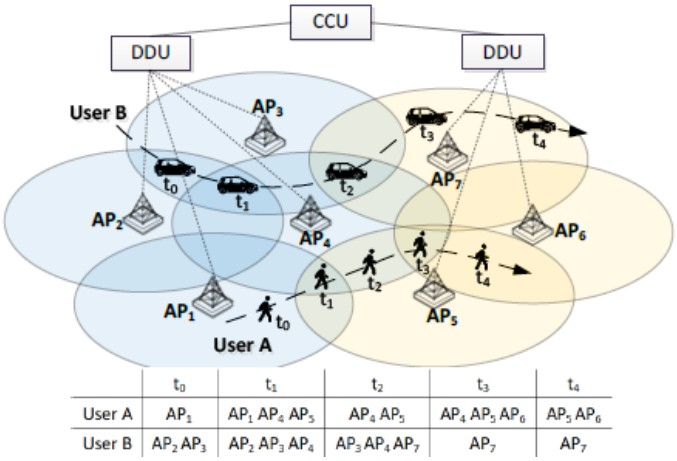


Figure 14: AP management.



	t_0	t_1	t_2	t_3	t_4
User A	AP_1	AP_1 AP_4 AP_5	AP_4 AP_5	AP_4 AP_5 AP_6	AP_5 AP_6
User B	AP_2 AP_3	AP_2 AP_3 AP_4	AP_3 AP_4 AP_7	AP_7	AP_7

Figure 15: AP dynamic adjustment.

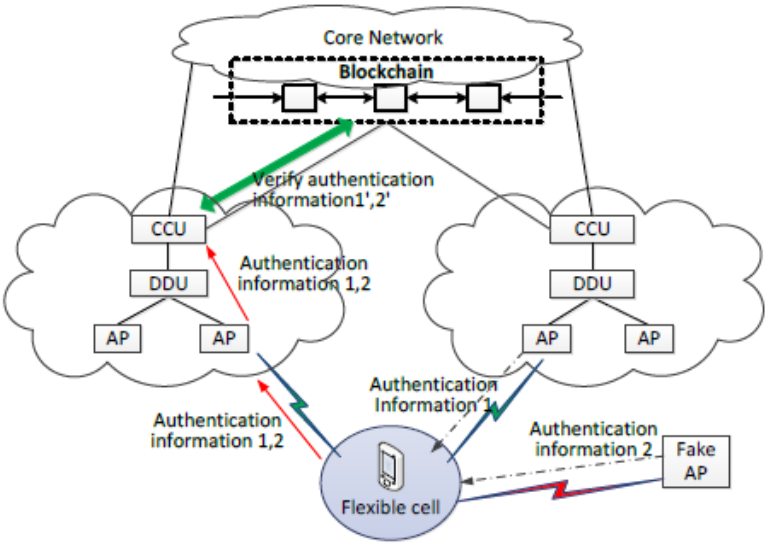


Figure 16: Authentication for access layer.

2.5 SAFE-6G Design Blueprint

SAFE-6G builds on three foundational planes of a distributed, open, user-centric 6G system: (i) Edge–Cloud Continuum Plane, (ii) Core Openness Plane, and (iii) User-centric Service/App Plane. These planes provide the basis for applying the requirements methodology and for enabling trust-aware adaptation through the SAFE-6G architecture.

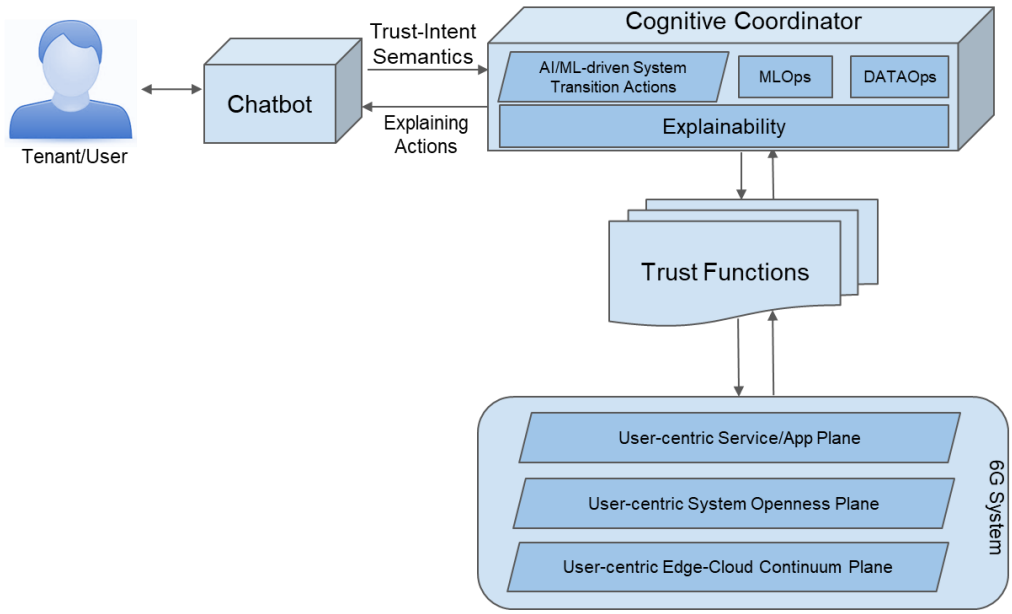


Figure 17: SAFE-6G design blueprint

Chatbot Domain: The Chatbot is the user's entry point to SAFE-6G. It collects user intent regarding the Level of Trustworthiness (LoTw) through natural-language interaction. The NLP component converts the user's input into structured data used by the Cognitive Coordinator. In metaverse pilots, the chatbot operates inside immersive environments and provides explainability (XAI) about the AI models involved in trust decisions.

Cognitive Coordinator Domain: The Cognitive Coordinator is a novel element of SAFE-6G framework, that orchestrates the five user-centric trust functions (safety, security, privacy, resilience, and reliability) across the distributed 6G edge-cloud continuum. It interprets user intents and translates them into trustworthiness scores which reflect the required level of trustworthiness. Those scores are derived by direct inference of its AI model while then it refines them to actual feasible, deployable scores by utilizing its Knowledge Base and Trust Function, resource-wise feedback. Finally, Cognitive Coordinator publishes those scores to the TFs, for them to proceed with the respective deployment actions and thus transforming the system into the requested trustworthiness state.

Trust Functions: SAFE-6G defines five AI-assisted trust functions—Safety, Security, Privacy, Resilience, and Reliability—that complement USN/NSN network functions and adapt across all lifecycle phases. **Safety** ensures resource isolation for USN/NSN deployments, protecting continuum resources from unauthorized access. **Security** safeguards sensitive data and system integrity through blockchain-based verifiable credentials, zero-trust principles, tokenized actions, and continuous vulnerability assessments. **Privacy** enables users to express privacy requirements via the chatbot, which then guide placement and resource-management decisions across the system. **Resilience** leverages AI-driven, intent-based network operations to sustain service continuity and dynamically adapt to changing conditions. **Reliability** integrates service and reliability profiling to detect anomalies and malicious behaviours, training ML models on resource and workload data to identify breaking points and perform real-time abnormality detection during execution.

SAFE-6G models the system using **three architectural planes**:

- **Service/App Plane**: Hosts personalized applications and vertical services that can interact with the network through exposed APIs.
- **6G Core Openness Plane**: Publishes programmable 6G core capabilities via OpenCAPIF standardized APIs.
- **Edge–Cloud Continuum Plane**: Supports distributed deployment of applications and network functions to optimize performance and user experience.

A key principle is that openness enables trust, so all planes expose their capabilities through CAPIF enabling the system to be adapted to the trust level required for each user.

The SAFE-6G **MLOps** and **DataOps** components work together to ensure efficient, reliable, and continuous AI model operation across the ecosystem. MLOps is responsible for the deployment, retraining, monitoring, and full lifecycle management of the AI models that support SAFE-6G functionalities, enabling consistent performance and rapid updates as system conditions evolve. Complementing this, DataOps focuses on providing and preparing raw data so that all information used for AI training and evaluation is accurate, consistent, and trustworthy. Together, they form the backbone of SAFE-6G's AI pipeline, ensuring that models operate on high-quality data and remain continuously optimized within the distributed environment.

2.6 Identification of Stakeholders and Roles

The following section describes an analysis of the stakeholders/actors and roles expected to interact directly or indirectly with the SAFE-6G ecosystem. A wide range of stakeholders and interested roles have been identified and grouped into related categories. Additionally, the analysis has been refined to address both the needs of the emerging 6G ecosystem and the unique requirements of the SAFE-6G framework. The evolution from network-oriented to application and user-oriented deployments is expected to introduce several modifications in the current identification of stakeholders and their roles.

- **Edge-Cloud Continuum Provider:** Organizations providing the necessary infrastructure and resources for the SAFE-6G framework to be effectively trained, deployed and monitored. This can be either one clusters that offers all the resources or a federation between different clusters acting, ensuring this way continuous service availability.
- **Edge-Cloud Continuum User:** Organizations that require high-performance computing, real-time data processing and low-latency communication for the purposes of SAFE-6G.
- **Core Network Provider:** It refers to a business entity that provides the core infrastructure, services, and technologies necessary for network operation, including managing data traffic, connectivity, and various network functions that comply with 3GPP standardization, such openness (e.g., CAPIF). Especially for the SAFE-6G ecosystem the core network provider shall support the proper interaction of the NFs (USN/NSN) with the Trust Functions, but also novelties and advances in the core network architecture, such as auxiliary NFs for resilient purposes etc.
- **MLOps Provider:** It refers to an entity that offers a platform for managing the machine learning lifecycle, from development to deployment and monitoring.

- **Chatbot Developer:** It refers to a professional or an entity who designs, builds, and maintains chatbot applications capable of interacting with final users in a conversational manner.
- **Chatbot Provider:** It refers to an entity that offers chatbot services to another organization or entity that needs a modern way for realising the human computer interaction interface either for data collection or for AI-assisted recommendations based on data that have been previously processed by the chatbot application.
- **Cognitive Orchestrator Provider:** It refers to an entity that offers a service that enables the orchestration and integration of AI models as well as the management of data pipelines and decision-making process automation. The SAFE-6G cognitive coordinator is understood as an intent-handling component that manages complex and abstract trust intent semantics, categorized into five taxonomies: Safety, Security, Privacy, Resilience, and Reliability. It determines the optimal goal state and orchestrates the five user-centric SAFE-6G functions to guide the transition of the 6G system towards this trusted state.
- **Cognitive Orchestrator Developers:** It refers to third-party entities or individuals aimed at creating, developing and implementing the orchestration computing algorithms and models that will support the realization of the Cognitive orchestrator module.
- **Trust Functions Developer:** Third-party entities or individuals interested in the development of their own SAFE-6G user-centric function for trustworthiness provision and have the opportunity to develop and integrate it as part of the SAFE-6G framework. By doing so, they can become part of a broader ecosystem for safe 6G networks. This approach not only enriches the diversity of available functions but also contributes to standardization efforts.
- **Trust Function Provider:** Any trusted third-party provider, which can offer a trust function for complementing the USN/NSN functionalities of the 6G core network.
- **Metaverse Provider:** Any third-party provider, who can offer a metaverse service provision.
- **Metaverse User:** Any tenant/user of a metaverse service/application over a 6G network.
- **Service User:** Any tenant/user of a generic service/application over a 6G network, usually without any trustworthiness requirements.
- **Mobile Network Operators (MNOs):** An MNO, also known as a mobile network provider or wireless carrier, is a telecommunications service provider that offers wireless voice and data communication services to its subscribers. MNOs own and manage the infrastructure necessary to deliver these services, including radio spectrum licenses, base stations, and the core network. SAFE-6G is a framework that can be adopted by MNOs and be offered to their customers (users, tenants, third party applications).
- **Telecom Vendors (TVs):** Telecom vendors are entities that are building the necessary equipment needed to realise a telecom infrastructure.
- **Tier-1 suppliers (TSs):** Suppliers of the telecom vendors, dealing with the availability and offer of new components needed for telecom infrastructure.
- **Security service providers (SSPs):** It refers to entities that are offering to the market security services, among which SAFE-6G, which they will introduce it to the telecom market and commercialize it either as a Service or licensed for private deployments.
- **Open-source communities (OSC):** OS Communities initiate open-source projects in order to complement the SAFE-6G solution with additional features. Via this process, a new generation of developers will be trained for building trusted applications for 6G systems.

- **ICT application providers (IAPs):** Businesses and vertical providers interested in integrating and exploiting the capabilities of the SAFE-6G framework in order to enhance their applications or products. Although the framework is tested in two use cases, specifically focused on industrial applications and educational environments, its universality allows for its applicability across a wide range of scenarios.
- **Research and Technology Organisations (RTOs):** Interested stakeholders that will research and develop new AI models and algorithms that can enhance the performance and Level of Trust of the tenants and third parties.
- **Infrastructure Providers (InfP):** Infrastructure providers, who can form joint ventures with other infrastructure owners for providing as services their infrastructures for the realisation of the edge-cloud continuum and the user-centric distributed 6G system.
- **Standards Development Organization (SDOs):** An entity responsible for developing, coordinating, and maintaining standards in various industries. SDOs will receive inputs from SAFE-6G outcomes that will influence their requirements definitions, architectural evolution, security provisions and user/tenant/applications support.
- **Regulatory Bodies Organisations and Associations (RBOs):** These bodies define new regulations and guidelines for the provision and use of 6G trustworthiness frameworks, like SAFE-6G, regulating the market and proposing legislation frameworks to policy makers.

2.7 Identification of Stakeholders Concerns

A concern is a topic of interest to one or more stakeholders belonging to an architecture [13] . A concern could manifest in many forms, such as in relation to one or more stakeholder's needs, goals, expectations, responsibilities, requirements, design constraints, assumptions, dependencies, quality attributes, architecture decisions, risks or other issues pertaining to the system [14] .

The mentioned standards do not provide a comprehensive set of potential concerns nor prescribe they granularity, how they relate with others or with other statements about the architecture such as its goals or requirements. Still, the list of quality characteristics described by the ISO/IEC 25010:2023 standard can be considered as a starting point for designing architectures and systems' realizations. Since SAFE-6G devises a trustworthy framework around its SBA, all the listed concerns are of interest to one or many of the stakeholders involved (see Section 2.6). The described concerns are seen in the following diagram:

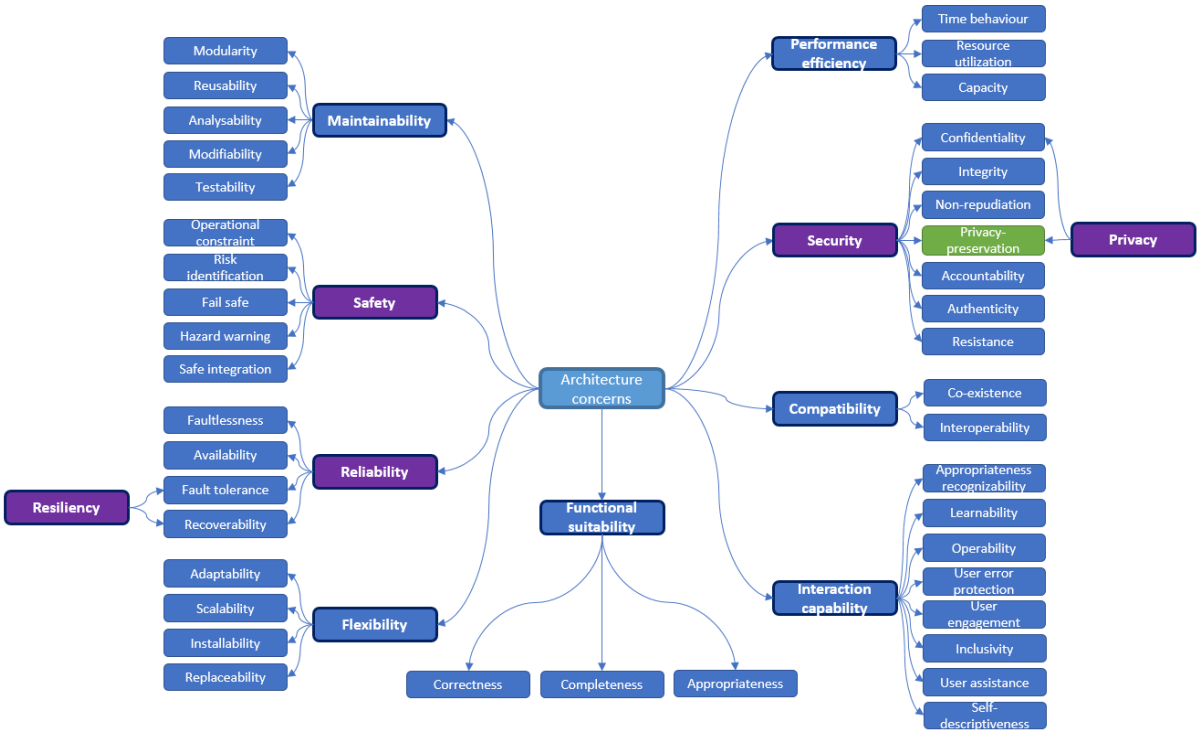


Figure 18: List of concerns.

The descriptions can be found in [14] , [15] . These concerns are being considered for building the different architecture views, to be reported in D2.2. The formalized requirements (see Section 5) can be related to one or some of these characteristics, with the **functional ones falling under the features of the functional suitability characteristic**. In any case, given the nature of the project (which targets trustworthiness, see Section 2.1), the SAFE-6G trust functions could be considered as functional, although due to their nature they could fall also under the security, reliability and safety categories (highlighted in purple), from an end-user perspective. Besides, mentioning also that privacy-preservation has been included within security, as the features included by the standard (mostly confidentiality) do not fully capture its related concerns.

Aiming at particularizing to the project's framework, the following **SAFE-6G specific concerns** are described, with the stakeholders they involved and their roles on each of them. It should be highlighted, again, that these concerns will be considered during the design of the architecture views (mostly the functional one):

#1: Considering the disaggregated computing continuum ecosystem spanning from Cloud/s to far and near Edges, owned by different stakeholders (multi-tenancy), new security and trustworthy challenges and risks are opened	
Concern from	• **Edge-Cloud continuum user:** More attack surfaces from geo-distributed locations means more possible attacks against 6G core functions and other services involved. • **Telecom vendors:** same concern but related to their offered 6G systems. • **MNOs:** same concern but extended to their offered networks.

	• **Chatbot provider, Metaverse provider, ICT application providers**: same concern but related to the potential sensitive data managed by the application. • **SDOs, RBOs:** New paradigms may pose at risk sensitive information or go against specific regional/country/European priorities.
Role (opportunity)	• **Cognitive orchestrator provider, SSPs:** To provide/ commercialise new solutions that help determine the LoT in specific parts of the system, so the system can make decisions based on users' intents considering contextual information from the different system components & AI. • **Trust Function Provider:** To provide dedicated functions and services to increase the level of security, privacy, safety, reliability and resiliency of the system, later considered by the providers above. • **InfP:** State-of-the-art cybersecurity mechanisms must be provisioned to minimize the risk from the infrastructure perspective. • **Edge-Cloud Continuum Providers:** Same role as above but applied to the considered mechanisms and technologies for managing the continuum, in terms of networking, data, identification and authorization of users and services. • **RTOs, OSC, Cognitive orchestrator developer, Trust function developer:** Research (RTOs mainly) and/or implement (open source or not) novel mechanisms that are later adopted by the stakeholders above. • **SDOs, RBOs:** To define trustworthy-related specifications/regulations, with respect to the different trustworthiness dimensions.

#2: Concern about how to deploy the system. Mechanisms that allow services to be easily created, placed, scaled and moved between continuum domains are needed in the novel distributed 6G core architecture	
Concern from	• **MNOs, Edge-Cloud continuum user:** The lifecycle of the considered virtualized software elements (trust functions, core, etc.) should be easy to manage in the hyper-distributed ecosystem. • **6G Core provider, TVs:** Concern of having to update their current offerings to cope with the new paradigm. • **Chatbot provider, Cognitive orchestrator provider, Trust function provider, Metaverse provider:** Concern to have a powerful, yet easy-to-use mechanisms to deploy, upgrade and scale their offerings in the distributed environment.
Role (opportunity)	• **Edge-Cloud continuum provider, MLOps provider:** Should provide user-friendly, efficient resources and service orchestration capabilities (including AI-related processes) to cope with this concern. • **SSPs:** May offer supporting features to the providers above, and work on commercialising the system.

#3: The dynamicity of the infrastructure will require openness to maximize the capabilities of the different providers in this changing ecosystem – as well as to unlock new core functions and use cases. This openness should encompass metrics and features from infrastructure, continuum and 6G core, with accessibility, usability and interoperability to be effective	
Concern from	• **Cognitive orchestrator provider, Trust function provider, Chatbot provider, ICT application provider:** Need access to data (current, historic) and exposed services from the 6G core, the continuum and the underlying platforms, to design adaptable, responsive trustworthy functions. • **Cognitive orchestrator developer, Trust function developer, Chatbot developer:** Same concern as above but extended with access to curated documentation, guidelines and best practices. • **MNOs:** Will require of additional monitoring and analytic tools to understand the behaviour of the platform and the involved systems, adapted to the new ecosystem.
Role (opportunity)	• **Edge-Cloud continuum provider, MLOps Provider:** Should provide both access and monitoring capabilities to the offered features, to cope with this concern and open new possibilities (as 6G core providers do via NEF). • **ICT application providers, RTOs, OSC:** This new paradigm facilitates the involvement of new actors, bringing new and/or enhanced concepts/features. • **SDOs:** Work on standardising interfaces (related to exposure and monitoring).

#4: All new features (in this case, related to trustworthiness) come with a cost in terms of computation, usability, agility and swiftness, that must be recognized and addressed. If performance is reduced, it will be difficult that stakeholders and users adopt the proposition	
Concern from	• **MNOs, Edge-cloud continuum user:** Will require of additional monitoring and analytic tools to understand the behaviour of the platform and the involved systems**.** Concerns about potential increase in resources needed. • **ICT application providers, Metaverse providers:** Final system should be accessible by non-experts, to have enable the use of the offered features for designing their applications**,** i.e., to configure the LoT based on the specific critically, risks and requirements of the use cases. • **Chatbot provider, Cognitive orchestrator provider, Trust function provider:** Similar concerns as above but related to the ease of deploying and maintaining their offerings rather than exploit the benefits of the trustworthy functions.
Role (opportunity)	• **Cognitive orchestrator developer, Trust function developer:** Should design functions that are efficient and effective, optimizing the use of resources. • **Edge-Cloud continuum provider, MLOps provider:** Orchestration mechanisms should allocate the trust functions in the proper way of the continuum, so they can provide their features with enough resources while aiming at minimizing their impact in the user experience. Also offering a good experience for the Cognitive framework, trust functions and chatbot providers.

#5: Standards must be supported but also expanded, as any proposition made on the telco domain, otherwise its long-term sustainability is on risk	
Concern from	• **MNOs, Telecom vendors, Tier-1 supplier:** Any new feature is always welcome and brings new opportunities but will not have much success (and thus, discarded) in the mid/long-term if it is not standardized. • **Cognitive orchestrator provider, Trust function provider, SSPs**: If the SAFE-6G system proposition lacks support from the standards, either working on or commercialising this kind of solutions would pose a risk for their financial sustainability. • **ICT application providers, 6G Core provider:** Applications should be built considering widely exposed resources to maximize their potential. These providers will not adapt their solutions to a system that does not show potential to be adopted or standardised, in case such adaptations are needed.
Role (opportunity)	• **Cognitive orchestrator provider, Trust function provider:** Once the SAFE-6G system has been validated, providers may want to foster standards aligned with their offerings. • **MNOs, 6G Core provider:** Embracing and fostering SAFE-6G in the standardisation arena could provide a mid- and long-term advantage against competitors, thanks to the added value the system brings. • **Edge-Cloud continuum provider, MLOps provider:** Although K8s is quite popular as VIM for telco operators, computing continuum and orchestration standards are yet immature. • **RTOs, OSC:** Could influence SDOs with the research and innovation actions carried out in the field. • **SDOs:** Trust (specially security and privacy) capabilities bring potential standardization opportunities, if they can protect users and critical data.

#6: AI cannot be used anymore as a black box that provides outputs without proper justification, especially when considering a trustworthy framework. Explanatory (and robust) approaches must be in place and accessible (example-based, feature-based, semantics-based) to offer confidence	
Concern from	• **MNOs, TVs:** As responsible for the system, they should understand the systems involved before offering it to external stakeholders. • **6G Core provider, ICT application provider, Metaverse provider:** If they consider the framework, outputs from AI processes must be understood by users and/or other systems, especially if have a direct effect in their offerings. • **RBOs:** New mechanisms using AI must follow existing European Union and national guidelines and regulations.
Role (opportunity)	• **Cognitive framework provider, Trust function provider, OSC:** Long-term sustainability and wide adoption of the provided features will largely depend

	on explainability capabilities of the AI processes involved, especially as key trustworthy aspects are managed. • **MLOps provider**: Solutions can help bridge the gap between the outcomes of the providers above and adopters (e.g., MNOs, ICT application providers, etc.) by providing a systematic approach to developing and deploying XAI models. • **Chatbot provider:** Could implement interfaces that presents the outcomes of the Cognitive orchestrator in a human-friendly way. • **RTOs**: Can explore, innovate and implement novel AI approaches that can be integrated as part of the SAFE-6G system or similar ones.

#7: Providing new features for the core network powered by AI requires a common way of managing the AI and Data operations, to standardize (and facilitate) their integration and avoid redundancy platforms for supporting their execution	
Concern from	• **Cognitive framework provider, Trust function provider, Metaverse provider, ICT application provider:** Having to manage the entire ML lifecycle as part of their solutions requires expanding their software or having to bring an external tool, increases the development and integration efforts (the latter two only in case of involving AI models in their offerings). • **MNOs:** If several modules involve ML pipelines, concern about potential redundancy of software managing MLOps and related processes.
Role (opportunity)	• **MLOps provider:** Can develop a framework to support the lifecycle of the AI processes and/or the data, offloading it to other providers and optimising the use of resources. • **RTOs, OSCs:** Could research and innovate on novel features and approaches to support the MLOps lifecycle management and orchestration, and influence SDOs with their outcomes. • **SDOs**: Opportunities for standardisation of AI processes could facilitate a system that involves many independent AI-powered modules, as happens in SAFE-6G.

#8: In this new hyper-distributed paradigm, with new actors, services and processes, attacks, errors or misconfigurations have the potential of affect the performance (e.g., service unavailability) of a system or affect sensitive data (e.g., privacy issues, data leaks). Accountability and privacy mechanisms must be provisioned to log critical data or events	
Concern from	• **MNOs, Telecom vendor, Edge-cloud continuum user:** Since new services are to be integrated in a more complex environment, which can affect different features of the system (news and existing ones), critical events must be immutably logged for accounting in case their operations affect the platform.

	• **6G Core provider, Cognitive framework provider, Trust function provider, Chatbot provider, InfP:** Similarly to the former, as some of their features/data will be exposed, accountability and traceability mechanisms are needed. • **Service user, ICT application provider:** If there is a leakage of key personal information, the mentioned mechanisms should be deployed to understand its potential impact.
Role (opportunity)	• **Edge-Cloud computing continuum provider, SSPs:** Can offer the required mechanisms for the rest of stakeholders, and log into them the key events of their specific features. • **RBOs, SDOs**: Regulatory aspects related to auditable processes could be defined, as well as standard interfaces to log them.

3 SAFE-6G USE-CASES HIGH-LEVEL OVERVIEW

To fulfil the validation objectives of the SAFE-6G framework, two metaverse use-cases will be deployed on a fully operational yet small-scale and prototype SAFE-6G framework for validating the user-centric 6G service provision [16] .

In this section, a high-level overview of proposed metaverse use-cases is thoroughly described. These use-cases are designed to illustrate and validate the feasibility and benefits of the SAFE-6G approach. The aim is to pave the way for new services that will flourish, ensuring the necessary trust in the system, which is crucial for user acceptance across various fields and sectors:

- **Use-case 1 is based on the Digital Twins (DTs) of an industrial production line**. DTs are indeed powerful tools for industries to mirror their existing installations and processes, enabling greater flexibility within factories and optimizing production times. 6G networks will play a central role in enhancing the trustworthiness of digital twins by providing users with reliable, resilient, secure, private, safe, real-time and comprehensive data exchange.

- **Use-case 2 aims to explore the capacities of 6G for a metaverse application for education.** Indeed, traditional hands-on learning methods require physical presence under the same location and experience is usually delivered through pre-defined scenarios where interaction is limited. The addition of sensing capabilities for learning scenarios where participants are in remote locations impose a significant challenge for 6G networks to ensuring secure online interactions and exchange of data.

SAFE-6G proposes a foundation of trust for 6G networks critical for the effective deployment of DTs across the manufacturing sector and education alike. Indeed, through the development of the two metaverse use-cases described in this section, SAFE-6G aims to demonstrate that “trustworthiness” can be something to be built upon the integration of capabilities expected for the next generation of 6G networks and third-party verticals and service providers. Both use-cases will also take full advantage of Extended Reality (XR) and AI technologies and will move beyond the typical XR-equipment, such as traditional VR/AR headsets. To do so, the use-cases will introduce novel sensing and capturing devices which optimize the user experience in virtual extended reality and motion capture applications.

In the following sections, first steps taken in the project to refine and enhance the originally proposed use-cases are presented. The final definition of the two metaverse use-cases will be detailed in Deliverable D2.3 at M12.

3.1 USE-CASE 1: INDUSTRIAL DIGITAL TWIN OF A PRODUCTION LINE

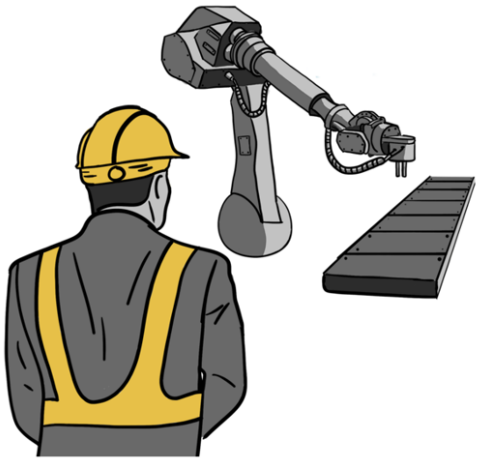
DTs are valuable tools that provide organizations with detailed insights into equipment performance, enabling predictive maintenance by identifying issues before they lead to costly breakdowns. Having a digital replica of a factory allows to gain flexibility, optimize production times by simulating scenarios and workflows and adapt more quickly to issues. This use-case will investigate how production teams

can leverage XR+AI services to maximize the potential of factory DTs, particularly in adapting and rescheduling machines and workers in response to emerging issues or changes.

The framework will be employed to visualize simulated 3D workflows and AI-generated machine/worker reorganization. Additionally, remote collaboration between users will allow decision-making based on these simulations and facilitate DT updates. In addition to the level of network performance required for the synchronization between their real and digital components, DTs also raise strong security and trust aspects. Safety, security, privacy, resiliency and reliability join sensitive and confidential factory data as crucial trust needs to be shared among different users through the network. Among others, Security risks directly involve the physical safety of workers, the production line machines and the overall production workflow of the factory. A holistic trustworthiness framework as SAFE-6G is proposing plays a pivotal role, primarily featuring on-premises services to be utilized and tested.

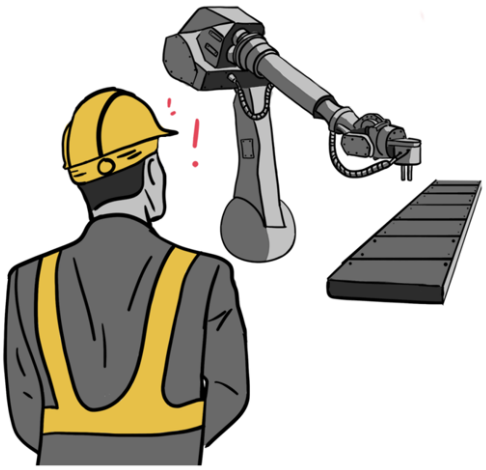
Scenario for Use-Case (UC) 1 is as follows: As illustrated in the following figures, UC1 builds upon the usage of XR+AI to solve an issue on the production line detected thanks to its DT. A large range of technical issues are possible, from the detection of defaults in the built products to signs of early wear and tear on machine components. In many cases, the production line needs to be interrupted and re-adapted to avoid physical injuries or harm on workers and factory equipment. A robust early detection or simulation tool thanks to a DT are thus valuable for factories.

When such an issue is detected, remote production managers are notified. These users will connect to the metaverse application using XR devices and the SAFE-6G network. Supported by the IMM IA agent (those from IMMERSION, partner of SAFE-6G), production managers can visualize the production line in XR, interact with 3D models of machines and equipment and simulate new workflows and production line designs to solve the issue. When a satisfying design is validated, the digital part of the DT is updated accordingly, which allows on-site technicians to perform the changes on the real production line.



1 A DT of a production line is running. Data from machines and workers can be monitored in real time or used to simulate scenarios for predictive maintenance.

Figure 19: Vision sketch of the first use-case – Step 1.



2 An issue is detected on the production line (for instance, machine component failure). A change in the production line is required.

Figure 20: Vision sketch of the first use-case – Step 2.

3 Production managers, at a remote location (elsewhere in the factory or in another site) are notified (phone/computer notification). They put on their XR equioment and connect to the DT application.

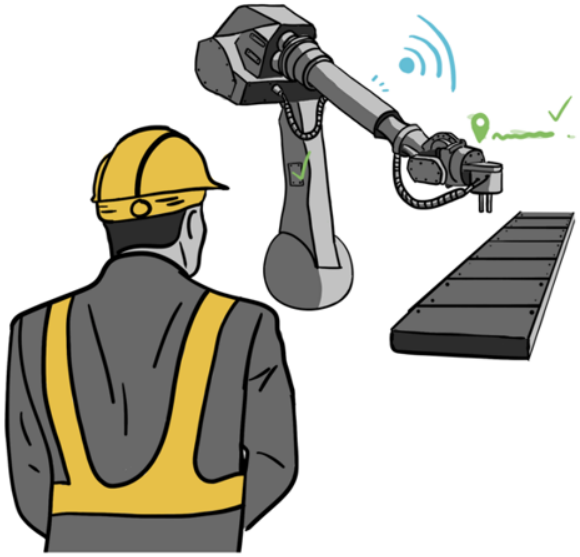
Figure 21: Vision sketch of the first use-case – Step 3.

4 Once authenticated, a production manager can visualize the production line in XR (at different scales and immersion levels) and check past/predicted incidents. He/she can adjust the production line setup and schedule while running simulations thanks to a specialized AI agent.

Figure 22: Vision sketch of the first use-case – Step 4.

5 The user validates the selected changes. The DT is updated and the real production line starts to synchronize itself.

Figure 23: Vision sketch of the first use-case – Step 5.



6 Production line managers monitor that the DT update are performed correctly, then ends the incident report. On-site workers handle changes in the real factory.

Figure 24: Vision sketch of the first use-case – Step 6.

3.2 Use-Case 2: Metaverse for Education

The availability of VR/AR devices and the shift to hybrid teaching during the COVID-19 pandemic inspired the creation of a hybrid classroom workspace, enabling both remote and on-site students to seamlessly participate in lessons and collaborative XR activities. The XR devices may indeed revolutionise education by creating immersive and interactive virtual learning environments. Students may explore complex subjects through simulations, enhances engagement with gamified content, and bridges the gap between theory and practice. This transformative approach makes learning more accessible, engaging, and effective, preparing students for the future.

The combination of XR+AI technologies, devices and solutions plays a pivotal role toto facilitate the transfer of knowledge and skill through real-time collaboration between on-site and remote users. On the one hand, XR allows groups of users to efficiently work on shared virtual 3D content, to simulate specific scenarios and repeat lessons and trainings to tailor the learning experience. On the other hand, AI agents can support both the teacher (for instance, by autonomously detecting which remote students need the most help) and the students (for instance, through conversational agents able to answer questions on the course when the teacher is not available).

An optimized network architecture is essential to deliver seamless learning and collaboration experiences. Current XR devices often lack 5G/6G compatibility, adding complexity to the deployment. Moreover, strong authentication and personal data security are crucial to protecting student and teacher information.

The scenario for the UC2 will implement a distributed network architecture combining edge and cloud computing to meet the real-time demands of hybrid education. It will be complemented by XR assets and IMM's collaboration software. The SAFE-6G framework's effectiveness in both scenarios will be evaluated across various deployment and placement options, focusing on safety, security, privacy, reliability, and resilience.

Too be precise, UC2, includes professional formation instead of student education only. This choice was motivated by several factors:

- Education and formation with XR+AI share many aspects, including but not limited to the transfer of knowledge and skill between remote users, telepresence, real-time collaboration and user privacy. While the course content may vary, many challenges remain the same.
- Formation also targets professional domains with more sensitive contexts and data. Security and trustworthiness, which are key aspects of SAFE-6G, are thus even more crucial than common teaching scenarios in schools.
- Including professional formation allows to consider scenarios with links to UC1 (for instance, a metaverse learning platform to train factory workers).

UC2 is therefore centred upon a XR+AI platform to teach factory technicians how to perform a maintenance procedure on a machine. This scenario is illustrated in the following figures. First, the instructor records in advance the procedure. At the beginning of the formation session, technicians connect to the metaverse application and can review the recorded procedure. Then, a more practical session allows them to train by virtually performing the procedure in XR while being supported by an IMM AI agent. At the end of the formation, technicians are certified on the procedure and able to perform it in the real factory.

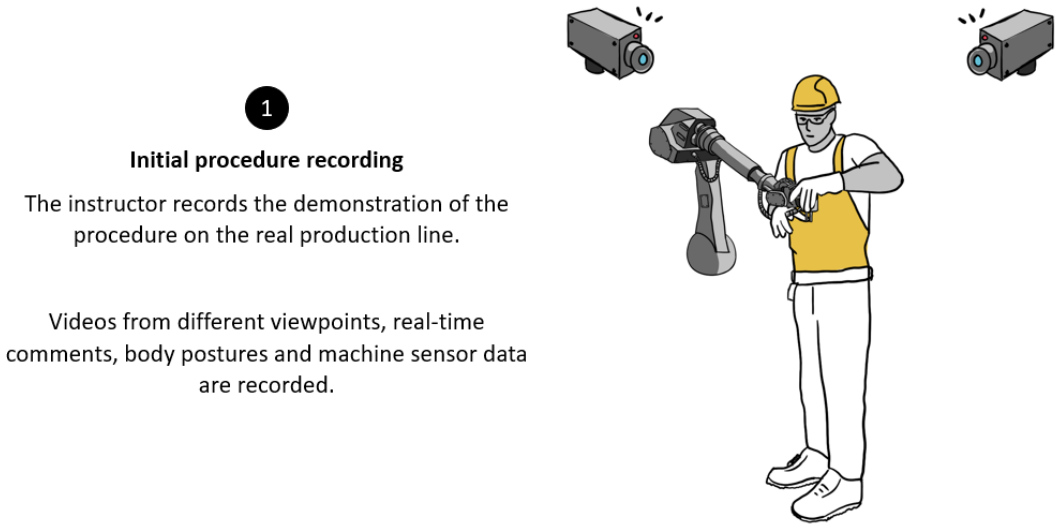


Figure 25: Vision sketch of the second use-case – Step 1

2

User connection

Technicians enter their formation room(s). They turn on their devices and connect them to the metaverse formation application using the Safe-6G network.

They authenticate themselves. The system checks that the appropriate person accesses to the formation (=> cannot make someone else pass the certification for you).

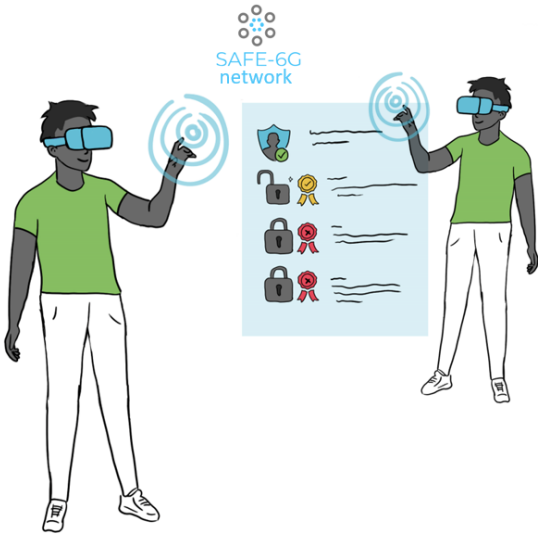


Figure 26: Vision sketch of the second use-case – Step 2

3

First learning phase

Technicians follow the recorded demonstration. Depending on their accreditation level, they have access to:

- Additional data (ex: body postures, factory sensor data…)
- Additionnal content (manual pages with detailed explanations, recordings of specific steps, etc).

They can ask questions to the IMM AI agent to get guidance and clarifications.

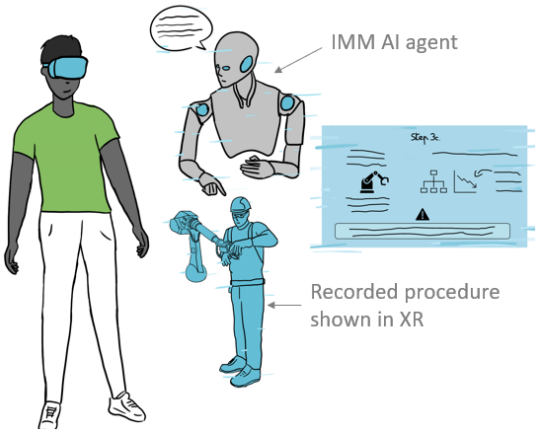


Figure 27: Vision sketch of the second use-case - Step 3

4

Practical training

Technicians are encouraged to train by performing the procedures and/or different scenarios in XR. To do so, they are divided in different XR spaces and work around hybrid replicas of the production line (hybrid replicas: some objects and tools are real but the rest is virtual).

The IMM AI agent support their training by providing real time feedback about the performed steps. In particular, the agent can correct gestures (comparing them to the instructor's gestures).

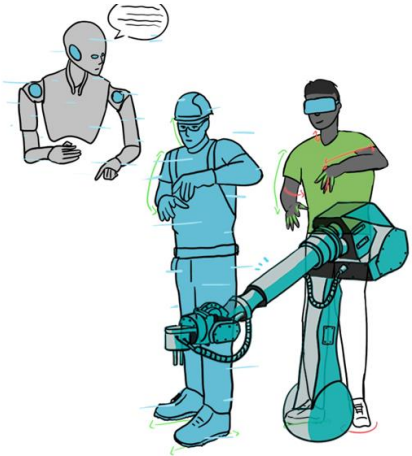


Figure 28: Vision sketch of the second use-case - Step 4

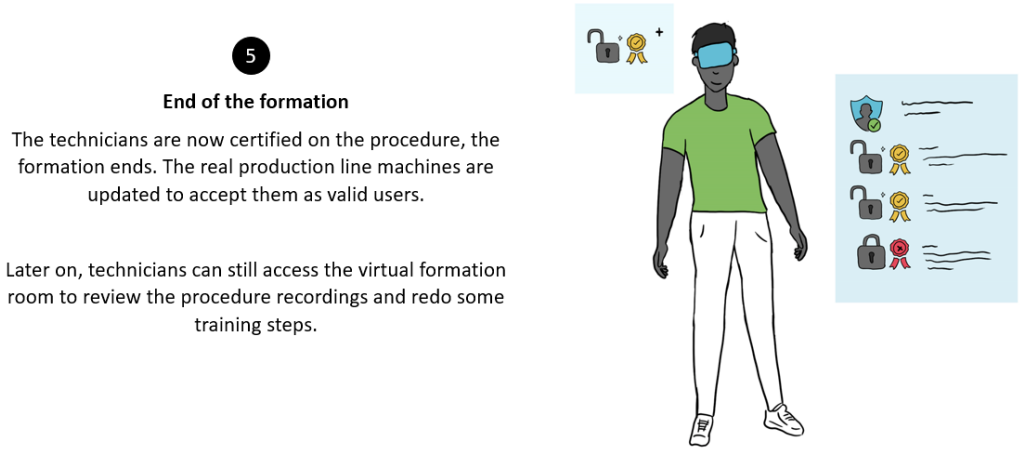


Figure 29: Vision sketch of the second use-case – Step 5

3.3 INITIAL INSIGHTS FROM USE-CASES

The first definition of the two use-cases was used to extract an initial set of insights and challenges from a trustworthiness perspective.

First, two types of AI agents can be defined. On the one hand, SAFE-6G AI agents are directly related to the SAFE-6G network components. They are thus fully part of the scope of the project, like for instance the SAFE-6G chatbot detailed in Section 5.2. On the other hand, IMM AI agents are only focused on supported the work of end-users (for instance, the one guiding the gestures of technicians in UC2). They are integrated within their respective metaverse vertical applications. Therefore, the IMM AI agents will appear in the use-cases but are out of the scope of the project.

At first sight, UC1 is the use-case with the most sensitive factory data in terms of resilience, reliability and security as it involves the whole environment of a running production line (machines, equipment setup and human workers). Principles of Zero-Trust architectures should be followed to ensure that users only have access to the relevant data. Punctual and contextual anomaly detection could be a way to monitor user behaviours and access requests to relevant data only (for instance, not downloading a large range of DT data from another production line for instance). Data breach detection would also be interesting in that regard. UC2 involves more simultaneous users and a larger range of XR devices. It thus raises concerns about privacy of users, security and safety of data (sharing the 3D environment, personal/behavioural or biometric data...).

In both use-cases, continuous authentication is also requested that only authorized users are accessing the metaverse application content. For instance, users should not be able to authenticate once, then give the XR headset to somebody else to visualize DT content (UC1) or pass the certification for them (UC2). Moreover, involved end-users may have different roles, locations, accreditations and devices. There is thus a strong need to define and assign different Levels of Trust to the different roles. Consequently, users with high Levels of Trust should be able to request adjustments on the fly for low Level of Trust users. This could be achieved through the SAFE-6G chatbot.

Finally, to better connect these initial insights with the SAFE-6G architectural design and the elicitation of technical requirements, we clarify that the initial needs identified in UC1 and UC2 are directly

addressed by the SAFE-6G Trust Functions. As described in the use-case analysis, UC1 stresses Security, Safety, Reliability, and Resilience due to sensitive factory data, asymmetric user roles and the need for continuous, stable XR collaboration, while UC2 emphasizes Privacy, Security and Safety due to the intensive use of XR sensors, sharing of 3D environments and the risk of cyber-physical attacks. The SAFE-6G architecture, through the five Trust Functions, explicitly complements these needs by ensuring secure access control and continuous authentication, protecting sensitive data streams, detecting anomalies, maintaining reliable and resilient service delivery, and enabling dynamic adjustments of trust levels via the SAFE-6G chatbot and the Cognitive Coordinator. More detailed and use-case-specific requirements will be further analysed in D2.3.

4 METHODOLOGY FOR THE TECHNICAL REQUIREMENTS

4.1 METHODOLOGY PRESENTATION

This section presents the methodology adopted for defining the technical requirements of the SAFE-6G system. The approach follows a user-centric and trust-driven analysis, ensuring that requirements reflect the diverse expectations, constraints, and operational needs of the stakeholders across the full 6G lifecycle. The methodology is grounded in the five user-centric trust functions—Safety, Security, Privacy, Resilience, and Reliability—which structure the requirements and ensure alignment with the core vision of native 6G trustworthiness. Furthermore, the requirements analysis process is driven by the project's use cases, which capture a broad range of technical, operational, and business-oriented scenarios. By deriving requirements from realistic and heterogeneous application contexts, the SAFE-6G framework ensures relevance, applicability, and completeness. The analysis further incorporates dependability, transparency, and trust-by-design principles, guaranteeing that the resulting requirements support a coherent, secure, and reliable architectural blueprint.

A structured and widely accepted practice for defining requirement strength in technical specifications is the terminology introduced by the IETF in RFC 2119 [17] . Although RFC 2119 uses its own controlled vocabulary ("MUST", "SHOULD", "MAY"), its underlying principles map directly to the requirement categories used in SAFE-6G. Following this model, Mandatory requirements correspond to RFC 2119 MUST/SHALL and define capabilities that are essential for correct operation and interoperability of the SAFE-6G framework. Recommended requirements align with RFC 2119 SHOULD/SHOULD NOT and describe behaviours that are strongly advised and expected to be implemented, unless specific justifiable conditions warrant deviations. Finally, Optional requirements align with RFC 2119 MAY/OPTIONAL and introduce features or behaviours that enhance the overall system but are not strictly necessary for baseline compliance. Using such categorisation ensures clarity, reduces ambiguity, and reflects best practices found in international standardisation activities.

In D2.1, we explicitly follow this structured requirement-strength model, categorizing all SAFE-6G requirements into Mandatory, Recommended, and Optional classes. This approach ensures consistency across domains and provides a clear prioritization scheme for the architectural design (D2.2) and subsequent implementation activities. By adopting a methodology aligned with the principle of RFC 2119, the SAFE-6G requirement set becomes more traceable, interpretable, and directly actionable for WP3, WP4 development and WP5 integration and validation.

To address the complexity and volume of the requirements, the methodology explicitly incorporates mechanisms that ensure their systematic translation into a coherent and feasible architecture. In particular, each requirement (prioritized as Mandatory, Recommended, Optional) is mapped to concrete architectural elements, interfaces, and system behaviours during the design process, ensuring that compliance drives architectural fulfilment. Furthermore, interdependencies, potential conflicts, and cross-component implications are analyzed and resolved through the Conflict Resolution component of the Cognitive Coordinator that will be analyzed further in the upcoming deliverables (especially D2.2 and D4.1), guaranteeing consistency across the 6G system, Edge–Cloud Continuum,

MLOps, Cognitive Coordinator, Chatbot, and Trust Functions. Lastly, an upcoming deliverable (D2.3) will include a dedicated section analysing the benefits of the SAFE-6G architecture for the use cases, where the linkage between use-case requirements, architectural components, and the overall requirement set will be further detailed and clarified. This traceable, prioritized, and conflict-aware methodology ensures that adherence to the requirements not only guides but also strengthens the feasibility and the internal consistency of the SAFE-6G architecture.

The defined technical requirements have been integrated in a dashboard (Excel file traceability requirement dashboard) for the sake of traceability and validation later in WP5. This file is presented in the figure below:

Id	Domain	Category	F/NF	Importance M/R/O	Short title	Description	Associated User requirement
REQ.COM.ETH.NF.M.01	Common	ETH	NF	M	Compliance with legal requirements on data protection	Protection of personal data in compliance to the GDPR and any other identified (European, national) legal requirement that is relevant to project scope, to enhance trust. In any task involving process personal data, the project will document (i) the details on the procedures to be implemented for data collection, storage, protection, retention and destruction and confirmation that the project will comply with the relevant national and European Union legislation, and (ii) the details on the informed consent procedures to be implemented.	
REQ.COM.ETH.NF.M.02	Common	ETH	NF	M	Conformance with the AI act	The project and the involved AI tools (from the cognitive coordination to the trustworthy functions and the MetaOS system) will follow the rules and comply with the novel European AI act, to minimize any unforeseen risk on the systems created.	

Figure 30: Traceability requirement dashboard.

This file will be used as a main reference for the SAFE-6G framework development, and the status of the requirements' fulfilment will be tracked and validated on a later stage by WP5.

The technical requirements evaluation is not addressed as part of the work of the WP2 "*Realisation Process, Requirements and Reference Architecture Design*", but across all the technical tasks, since the SAFE-6G framework implementation is a continuous engineering task carried out in the technical WPs developing the individual components (WP3 "*User-centric Distributed 6G Core over Edge-Cloud Continuum with MLOps*" and WP4 "*AI-driven 6G Trustworthiness Functions and Cognitive Coordination*"). The component testing will be done at the corresponding WP, while the integrated component validation will take place in WP5-Integration, validation, and pilots, which is the WP integrating the components in the use cases and assessing the user acceptance.

4.2 Definition and Organization of the Requirements

The methodology followed for the definition, prioritization, and refinement of technical requirements of the SAFE-6G framework is based on extensive exchanges between all project partners (technical and end-users) during WP2 weekly meetings and other meetings that allow to:

- Define a list of the different stakeholders that will be concerned by the SAFE-6G framework (see Section 2.6 and Section 2.7).
- Understand end-users needs and in particular regarding their required level of trustworthiness (see Chapter 3 above).
- Build a blueprint of the future system architecture defining the different domains/components of the system (see Section 2.5 above).

The interest of this process is to cover the entirety of the reference architecture, without overlapping between domains. Moreover, even if the use case requirements will be defined more precisely later

in the project, one section has been added in this deliverable to propose some requirements derived from the use cases, which bring more depth to the technical requirements definition. Discussions among partners allowed highlighting the different synergy existing between Technical and User Requirements (technical requirements being in support of attainment of user requirements coming from the targeted use case & scenarios).

The technical requirements have then been structured and classified in the following way:

- A first level of classification with the different domains that have been identified in the blueprint architecture.
- A second level of classification with categories that have been defined for some large "encompassing" domains (like MLOps or cognitive coordinator) to focus on specific subcomponents of the domain.
- A third level of classification splitting requirements into functional and non-functional requirements:
    - Functional requirements define the essential capabilities, behaviours, and processes that the system must provide. They capture the concrete actions, interactions, and technical features expected by different stakeholder groups, effectively reflecting the aggregated needs of end-users, operators, developers, and domain experts. These requirements describe the operational scope of the system and ensure that all core functionalities of the SAFE-6G blueprint are explicitly defined.
    - Non-functional requirements, by contrast, describe the quality attributes that govern the system's operation rather than its specific functions. They define the conditions under which the system must perform and include characteristics such as performance efficiency, usability, interoperability, scalability, maintainability, and deployment constraints across the edge–cloud continuum. These requirements ensure that the SAFE-6G system not only performs its intended functions but does so in a trustworthy, robust, and user-centric manner.
- A last level of classification regarding the prioritisation of the technical requirements, to define each requirement's criticality:
    - **Mandatory ("Must-have")**: A label used for the most critical requirements which, if not delivered, could prevent the implementation.
    - **Recommended ("Nice-to-have")**: Denotes requirements that are important but not critical for the success of the implementation meaning they can be considered as features that add value without being essential. Such requirements can be less time-critical than "Mandatory" requirements or there might be alternative ways to satisfy them.
    - **Optional**: This category includes requirements that are desirable but not necessary. They are not necessary for the core functionality or success of the implementation but can be implemented if time and resources permit. They usually include aspects related to user experience or customer satisfaction which can be implemented if time and resources permit it.

To address the complexity and volume of requirements, the SAFE-6G methodology explicitly links each requirement to the architectural blueprint, ensuring clear traceability from stakeholder needs to concrete architectural elements. This structured classification demonstrates how fulfilling these requirements leads to a coherent, feasible, and implementable architecture.

4.2.1 Requirement template definition

To ensure a comprehensive and organized approach to identifying and categorizing all technical requirements defined by SAFE-6G partners, a template which is shown below was developed. This structured format aims to streamline the documentation process, facilitating easier management and reference of technical requirements throughout the project's lifecycle. Each element of the table is designed to provide a clear and detailed information that supports effective communication and coordination among all the project partners. The different items of the table are defined as follows:

- **ID**: Allows to clearly and uniquely identify each technical requirement.
- **Domain**: Based on the project's framework architecture and use cases, the main domains to which the requirements are related were targeted. This makes it easier to quickly identify potential synergies between different technical requirements.
- **Category**: Serves as a sub-domain, to specify particular aspects of the domain.
- **Requirement Type**: Indicates if the technical requirement is considered as "Functional" or "Non-Functional". Functional requirements define all the features and functions of the delivered framework that the final user can expect. Non-functional requirements describe the general properties of the system, how it will provide the services to meet the expectations set by functional requirements.
- **Priority**: Indicates the level of need for each requirement (Mandatory, Recommended, Optional).
- **Short title**: Provides a meaningful and not too long title that characterizes the requirement.
- **Description**: A brief text explaining the requirement, identifying the potential challenges and the objectives.
- **Associated User Requirement**: Provides, when it has already been identified, a particular interest to associated User Requirements for the use cases that will be implemented. SAFE-6G deliverable D2.3 will detail the use cases, as well as identified user requirements coming from use case scenarios.

4.2.2 Domain-Specific Application of the Template

The SAFE-6G requirements have been systematically split and classified into well-defined architectural components and domain-specific groups, as presented in the sections below. This structured organisation enables clear mapping between each requirement and the subsystem responsible for its fulfilment. We also acknowledge that, given the high number and diversity of requirements, potential conflicts may arise between architectural components during implementation. To address this, the Cognitive Coordinator includes a dedicated conflict-handling mechanism designed to detect, analyse, and mitigate such inconsistencies by leveraging Trust Function feedback, system context, and feasibility constraints.

This section illustrates how the requirement template is adapted to different domains within the SAFE-6G framework. Each domain uses the same template, but the interpretation and focus differ depending on the functional role of the domain:

Common Requirements Domain

These requirements apply horizontally to the entire SAFE-6G system and form the baseline for all other domains.

Template field	Description
ID	A unique ID in the form REQ-COM-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = COM**
Category	**CATEGORY = ETH | DES| RES** ETH: Ethics, legal and regulatory aspects RES: Resources DES: Design principles
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Chatbot Requirements Domain

Template field	Description
ID	A unique ID in the form REQ-CHAT-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = CHAT**
Category	**CATEGORY = TRU | XAI | ADA | UI | IME | DAT** TRU: Trust Level/Trustworthiness XAI: Explainable AI ADA: Adaptability UI: User Interface IME: Immersive Environments DAT: Data exchange endpoints
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional

Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Cognitive Coordinator Requirements Domain

Template field	Description
ID	A unique ID in the form REQ-COG-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = COG**
Category	**CATEGORY = KBASE | REAS | SCHED | AISER | PROG | FRA** KBASE: Knowledge Base REAS: Reasoning engine SCHED: Service and Function Scheduling AISER: AIaaS/FL/ML PROG: Programmability FRA: SAFE-6G Framework
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Safety Trust Function Domain

Template field	Description
ID	A unique ID in the form REQ-FSAF-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = FSAF**
Category	**CATEGORY = DES | COM** DES: Design COM: Communication
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional

Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Security Trust Function Domain

Template field	Description
ID	A unique ID in the form REQ-FSEC-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = FSEC**
Category	**CATEGORY = NET | INT | PER | COMP** NET: Network INT: Interoperability PER: Performance COMP: Compliance
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Privacy Trust Function Domain

Template field	Description
ID	A unique ID in the form REQ-FPRI-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = FPRI**
Category	**CATEGORY = PSC | DSS | GEN** PSC: Privacy Score Calculation DSS: Decision Support System GEN: General
Requirement type	**Requirement type = F | NF**

	F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Resilience Trust Function Domain

Template field	Description
ID	A unique ID in the form REQ-FRES-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = FRES**
Category	**CATEGORY = NET | FRA | INFRA | DATA** NET: Network FRA: SAFE-6G Framework INFRA: Infrastructure DATA: Data
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary.
Associated user requirement	List the associated User requirement

Reliability Trust Function Domain

Template field	Description
ID	A unique ID in the form REQ-FREL-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = FREL**
Category	**CATEGORY = RES | NET | AI** RES: ResourcesNET: Network AI: Artificial Intelligence
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional

Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

MLOps Domain

Template field	Description
ID	A unique ID in the form REQ-MLOPS-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = MLOPS**
Category	**CATEGORY = XAI | DEV | TRAIN | DP | DT | MLLIB | INF** XAI: XAI DEV: Pipeline Development TRAIN: Model Training DP: Differential Privacy DT: Digital Twin MLLIB: ML Model Library INF: Inference phase
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

User Centric Distributed 6GCore Domain

Template field	Description
ID	A unique ID in the form REQ-UCEN-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = UCEN**
Category	**CATEGORY = DES | COMP** DES: Design COMP: Compliance
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional

Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

Edge-Cloud Continuum Infrastructure Domain

Template field	Description
ID	A unique ID in the form REQ-INFRA-CATEGORY-TYPE-PRIORITY-#
Domain	**DOMAIN = INFRA**
Category	**CATEGORY = RES | META | SEC | NET** RES: Resources META: MetaOS-related SEC: Security NET: Network
Requirement type	**Requirement type = F | NF** F: Functional NF: Non-Functional
Priority	**Priority = M | R | O** M: Mandatory R: Recommended O: Optional
Short title	A meaningful and not too long title that characterizes the requirement
Description	General description, a brief text explaining the requirement, including the objectives where necessary
Associated user requirement	List the associated User requirement

5 FRAMEWORK FUNCTIONS/COMPONENTS AND DERIVED REQUIREMENTS

5.1 COMMON SYSTEM REQUIREMENTS

5.1.1 INTRODUCTION

SAFE-6G system will contain several modules leveraging AI models and related technology. Being a framework that aims at contributing towards increasing the trustworthiness of 6G systems, it is crucial that its AI-assisted components are robust and trusted by potential adopters. Thus, SAFE-6G's view on this involves creating models for each one of the trust functions that are in turn reliable, secure, safe, resilient and privacy-respectful. To that end, SAFE-6G will consider the following approach for designing and implementing its AI-driven modules:

- First, from the legal and ethical perspective, partners will ensure compliance with current and future regulations concerning involved aspects – not only the AI act, but also relevant European directives such as the Data act and GDPR, when applicable.
- For the sake of transparency and interpretability, XAI will be fostered, preventing the implementation of a system which outputs are hard to understand and interpret and thus ensuring that the system is intuitive and easy to use.
- From the technical viewpoint, although SAFE-6G partners are experts in the involved domains, the Consortium will pay close attention on available results of the European and Open-source research communities, to align with novel AI trends and recent results.
- Standard approaches like MLOps or Federated Learning (FL) will be applied when possible and adapted with the natural evolution of involved technologies. Also, special care must be put on data quality, as typical part of the AI pipelines. Data quality assessment strongly depends on the type and scope of the data handled, so aspects such as correlation, dimensionality, PCA, median, quartiles, etc. will be studied, as otherwise the performance of the models can be hindered.

To support all the processes and facilitate its potential adoption by the 6G ecosystem, the system design should comply with key 5G and beyond standards as well as aligning with modern computing paradigms (IoT-edge-cloud, Cloud Native). Also, the extensive use of AI demands having enough (computing/acceleration, networking and storage) resources to perform, access to relevant data (historic and real-time) and as close to their sources as possible to minimize the energy related to their transport. The latter, along with designing efficient (e.g., frugal) models and leveraging techniques like FL, contribute towards optimal usage of resources, and thus towards SAFE-6G's long-term sustainability. Following all the previous rationale, this section presents a set of requirements that should guide the design of SAFE-6G architecture and the development of its modules.

5.1.2 COMMON SAFE-6G SYSTEM REQUIREMENTS

ID	REQ-COM-RES-F-M-01
Short title	Holistic trustworthy approach

Description	SAFE-6G aims at implementing a trustworthy framework to support and enhance the trust over the next evolution of the cellular network and the managed resources. In turn, it is key for its potential adoption that this framework is also considered secure, safe, reliable, resilient and privacy-respectful, implementing dedicated mechanisms and leveraging its own ones for that aim.
AUR	N/A

ID	**REQ-COM-DES-F-R-02**
Short title	AI-driven trustworthy functions
Description	Each function and component of SAFE-6G must have been designed and developed with an internal AI-assisted module in order to optimize independently its functionality and decisions.
AUR	N/A

ID	**REQ-COM-ETH-NF-M-03**
Short title	Compliance with 5G and industry standards
Description	Involved SAFE-6G components should leverage standards, when possible, to maximize its adoption potential. New features or components not yet subject to standardization are exempt.
AUR	N/A

ID	**REQ-COM-DES-F-M-04**
Short title	Following Cloud Native paradigm
Description	The modules and components of the system should be designed and developed following Cloud Native principles, this based on microservices, containers, CI/CD and DevOps.
AUR	N/A

ID	**REQ-COM-ETH-NF-M-05**
Short title	Conformance with the AI act
Description	The project and the involved AI tools (from the cognitive coordination to the trustworthy functions and the MetaOS system) will follow the rules and comply with the novel European AI act, to minimize any unforeseen risk on the systems created.
AUR	N/A

ID	**REQ-COM-DES-F-M-06**
Short title	Functions Virtualization
Description	The USN, NSN, Trust functions must be containerized and deployed in the virtualised environment of the SAFE-6G infrastructure.

AUR	N/A

ID	**REQ-COM-RES-F-M-07**
Short title	Data availability
Description	Sufficient amount of data should be available for the training of AI/ML models.
AUR	N/A

ID	**REQ-COM-DES-F-M-08**
Short title	APIs interaction through Open CAPIF
Description	SAFE-6G system will consist of several domains, each of them with different modules and APIs. Aiming at homogenising the exposure and consumption of the features of such domains, APIs of relevant domains (e.g., 6G Core, metaOS, MLOPs, cognitive coordinator, etc.) will be published and consumed primarily through it.
AUR	N/A

ID	**REQ-COM-DES-F-R-09**
Short title	Interface to MLOPS framework to train and execute ML models
Description	The ML methods based on the specific details of the task that is to be solved, e.g., number of input features, number of samples, will require interfacing with the MLOps framework in order to gain access to the needed resources, e.g. storage, computational power.
AUR	N/A

ID	**REQ-COM-DES-F-M-10**
Short title	CAPIF registration to interact with other SAFE-6G components in the framework
Description	Trust functions will be registered as provider/invoker in CAPIF to expose and/or consume data through APIs exposed from other SAFE-6G components.
AUR	N/A

ID	**REQ-COM-DES-F-M-11**
Short title	Supporting Infrastructure
Description	The SAFE-6G infrastructure layer must support containerization technologies, such as Docker and Kubernetes, for the realisation of the user-centric 6G network.
AUR	N/A

ID	**REQ-COM-DES-F-M-12**
Short title	Interoperability Requirement
Description	All functions must be able to interact seamlessly with other SAFE-6G components in the framework. This includes data exchange, synchronization, and error handling.
AUR	N/A

ID	REQ-COM-RES-F-M-13
Short title	Efficient AI models
Description	The system will target efficient AI algorithms, so that consumption of energy is not excessive. This is needed given the large number of models that will be involved, and their distributed nature.
AUR	N/A

ID	REQ-COM-ETH-NF-M-14
Short title	Compliance with legal requirements on data protection
Description	Protection of personal data in compliance to the GDPR and any other identified (European, national) legal requirement that is relevant to project scope, to enhance trust. In any task involving process personal data, the project will document (i) the details on the procedures to be implemented for data collection, storage, protection, retention and destruction and confirmation that the project will comply with the relevant national and European Union legislation, and (ii) the details on the informed consent procedures to be implemented.
AUR	N/A

ID	REQ-COM-RES-NF-M-15
Short title	Provisioning of processing resources
Description	Enough processing capabilities must be provisioned for supporting the services and processes to be managed by the framework, especially those related to AI (e.g., to train the AI models – possibility of using HPC, to run the AI models, to deploy the Cognitive Coordinator and the MLOps module).
AUR	N/A

ID	REQ-COM-DES-NF-O-16
Short title	GitOps Monitoring Requirement
Description	SAFE-6G components should be monitored through GitOps to manage and track changes. This includes version control, rollback capabilities, and audit trails.
AUR	N/A

ID	REQ-COM-DES-F-M-17
Short title	API Consumption Requirement
Description	Trust functions must be able to consume data through APIs exposed by other SAFE-6G components via CAPIF. The function should handle different data formats and ensure data integrity during consumption.
AUR	N/A

ID	REQ-COM-RES-F-M-18
Short title	Local processing capabilities
Description	SAFE-6G modules must exploit the distributed computing capabilities of the continuum, processing relevant/sensitive information at the edge and deciding which information needs to be transmitted to a central location for storage or further processing; thus, minimizing the size of the transmissions.
AUR	N/A

ID	REQ-COM-DES-F-M-19
Short title	Access to performance metrics from 5G/6G core infrastructure
Description	Access to monitoring data collected from the 5G/6G infrastructure, e.g., from NWDAF, CNC, UPF, is a must in order to feed the functions to train the ML methods and perform the required estimations.
AUR	N/A

ID	REQ-COM-DES-F-M-20
Short title	Access to performance metrics from the cloud continuum
Description	Access to monitoring data from the edge-central cloud is needed in order to feed all functions to train the ML methods and perform the required estimations.
AUR	N/A

ID	REQ-COM-DES-F-M-21
Short title	Access to performance metrics from user application
Description	Access to monitoring data collected from the user application, e.g. number of frames, service time, service availability etc. is a must in order to feed the functions to train the ML methods and perform the required estimations.
AUR	N/A

ID	REQ-COM-DES-F-R-22
Short title	The monitoring framework should support the streaming of monitoring data
Description	The Reliability function should be able to collect specific monitoring metrics in near real time during the inference phase using a publish-subscribe approach.
AUR	N/A

ID	REQ-COM-DES-F-M-23
Short title	Functions Scalability
Description	Each function of the evolved core network, namely (NSN, ISN, Trust Functions) must be able to scale themselves up if needed in order to properly support the specific user session.

AUR	N/A

ID	REQ-COM-DES-F-R-24
Short title	Fault Tolerance
Description	Each function and component of SAFE-6G must have been designed and developed in such a way that is capable of providing high fault-tolerance against failure of the system.
AUR	N/A

ID	REQ-FREL-DES-NF-R-25
Short title	High availability applications
Description	The user applications must support management actions (e.g., scaling up, scaling down, migration, etc.) to ensure the service's high availability based on the events coming from the reliability function.
AUR	N/A

ID	REQ-COM-RES-NF-M-26
Short title	Data persistence
Description	SAFE-6G roots on AI, which requires data, algorithms and models. Enough storage resources must be in place to ensure that relevant data, algorithms and trained models can be stored in the (distributed) system. Also, system design must consider the realization of the framework in real environments.
AUR	N/A

ID	REQ-COM-DES-F-M-27
Short title	Easy Maintainability
Description	Each USN/NSN/Trust function should be designed for ease of maintenance and updates, facilitating quick resolution of issues and incorporation of improvements or new security features.
AUR	N/A

ID	REQ-COM-DES-F-M-28
Short title	User-Friendly Interfaces
Description	The Trust functions' interfaces, both for administrators and users, should be intuitive and user-friendly to ensure correct implementation and management of security measures.
AUR	N/A

5.2 CHATBOT REQUIREMENTS

5.2.1 INTRODUCTION

The SAFE-6G project introduces an innovative trust framework for distributed human-centric 6G systems. A central component of this framework is the AI-assisted NLP-based virtual assistant/chatbot. This chatbot acts as an interface between users and the SAFE-6G system, enabling users to specify their intents and requirements related to safety, security, privacy, resilience, and reliability in an intuitive manner. The chatbot can also be integrated into XR/AR/MR environments, enhancing user experience in industrial production lines and education scenarios.

The chatbot application for the SAFE-6G framework must include several key functionalities to ensure effective user interaction and data processing. Firstly, it should provide a user-friendly interface that engages users with service-driven prompt questions tailored to gather specific requirements across the five SAFE-6G functions: safety, security, privacy, resilience, and reliability. The chatbot must capture user responses in real-time and convert these unstructured inputs (user intents & needs about the network) into structured data using NLP techniques. It should then employ Natural Language Understanding (NLU) and classification models to accurately recognize and categorize user intents.

Additionally, the chatbot must be capable of extracting relevant data points from user responses, ensuring the structured data is ready for further analysis by the cognitive coordination components of the SAFE-6G system. This comprehensive approach ensures that the chatbot can dynamically adapt to user needs and maintain high levels of trust and functionality.

Key Functionalities:

- User Interaction and Trust Level Computation:
  - The chatbot interacts with users through a conversational interface, utilizing advanced NLP techniques to parse and recognize user intents accurately.
  - It communicates these intents to the Cognitive Coordinator, which computes the required level of trust across various dimensions.
- Explainable AI Integration:
  - The chatbot provides clear explanations for the trust levels computed by the SAFE-6G system, complying with GDPR requirements.
  - Explanations can be delivered in various formats, ensuring users understand AI-driven decisions.

Technical Capabilities:

- Adaptability: Handles diverse user requirements and various use cases.
- User-Centric Design: Ensures accessibility and comprehensibility for non-technical users.

By incorporating this AI-assisted virtual assistant/chatbot, the SAFE-6G project aims to enhance trustworthiness and transparency in 6G systems.

5.2.2 CHATBOT REQUIREMENTS

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the chatbot component, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-CHAT-UI-NF-R-01
Short title	User-Centric Design
Description	The chatbot should be designed to ensure accessibility and comprehensibility for non-technical users, providing a seamless user experience.
AUR	Users need an easy-to-use interface that does not require technical expertise to interact with.

ID	REQ-CHAT-TRU-F-M-02
Short title	Trust Level Computation Integration
Description	The chatbot must be able to communicate recognized user intents to the cognitive coordinator, which will compute the required level of trust across various dimensions such as safety, security, privacy, resilience, and reliability.
AUR	Users require accurate computation and adjustment of trust levels based on their inputs.

ID	REQ-CHAT-UI-F-M-03
Short title	Conversational Interface for User Interaction
Description	The chatbot must provide a user-friendly conversational interface for interacting with users. This interface should utilize advanced NLP techniques to accurately parse and recognize user intents related to safety, security, privacy, resilience, and reliability.
AUR	Users need an intuitive way to communicate their requirements to the SAFE-6G system.

ID	REQ-CHAT-XAI-F-M-04
Short title	Integration of Explainable AI
Description	The chatbot must integrate XAI functionalities to provide users with clear explanations for the trust levels computed by the SAFE-6G system. Explanations should comply with GDPR requirements and be available in various formats such as textual or visual.
AUR	Users need to understand the AI-driven decisions affecting their trust levels.

ID	REQ-CHAT-ADA-NF-M-05
Short title	Adaptability to User Requirements
Description	The chatbot must be adaptable to diverse user requirements and various use cases. This includes handling different inputs and providing appropriate responses based on user intents.

AUR	Users need the chatbot to be flexible and capable of handling various scenarios and inputs.

ID	**REQ-CHAT-UX-F-R-06**
Short title	Automated Response Generation
Description	The chatbot should be capable of generating automated responses based on predefined templates and user input, enhancing interaction efficiency.
AUR	Users require timely and efficient responses to their queries.

ID	**REQ-CHAT-IME-F-M-07**
Short title	Integration with XR/AR/MR Environments
Description	The chatbot must be capable of integrating with XR/AR/MR environments to enhance user experience in industrial production lines and education scenarios.
AUR	Users in immersive environments need to interact with the chatbot seamlessly to enhance their experience.

ID	**REQ-CHAT-DAT-F-M-08**
Short title	Endpoints for Data Exchange with Metaverse Application
Description	The chatbot should expose and access endpoints to facilitate data exchange with metaverse applications. This includes receiving end-user inputs, requesting data from metaverse applications, and sending responses back to end-users. These endpoints ensure seamless integration without the chatbot directly handling XR input and output interactions, which will be managed by the metaverse applications.
AUR	Users need the chatbot to interact efficiently with metaverse applications to provide a cohesive experience.

ID	**REQ-CHAT-DAT-F-M-09**
Short title	API Interface for Cognitive Coordinator Communication
Description	The chatbot must include an API to communicate with the cognitive coordinator. This interface will allow the chatbot to send user intents and receive computed trust levels and other relevant data. The API must be designed to handle high-frequency requests and ensure data integrity and security.
AUR	Users require reliable communication between the chatbot and the cognitive coordinator to accurately compute and adjust trust levels.

ID	**REQ-CHAT-DAT-F-M-10**
Short title	Endpoint for Explainable AI Requests
Description	The chatbot should provide an endpoint to request XAI information.
AUR	Users need clear explanations for AI-driven decisions.

ID	REQ-CHAT-TRU-NF-R-11
Short title	Chatbot's High Availability
Description	In line with REQ-FREL-DES-NF-R-21, the chatbot must ensure a minimum uptime of 99.5%, ensuring reliable access for users.
AUR	Users need the chatbot to be available whenever their Level of Trust to the 6G Network requires to interact with it.

ID	REQ-CHAT-TRU-NF-M-12
Short title	Chatbot's High Performance
Description	The chatbot should perform efficiently under various loads, ensuring quick response times and smooth operation.
AUR	Users need the chatbot to function efficiently without delays.

5.3 Cognitive Coordinator Requirements

5.3.1 Introduction

The Cognitive Coordination component within the SAFE-6G ecosystem is essential for ensuring that the system meets the required LoT through management of AI and reasoning activities. This section outlines the specific requirements necessary for the cognitive coordinator to function effectively, focusing on how these requirements support the generation and refinement of trustworthiness metrics.

5.3.2 Cognitive Coordinator Requirements

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the Cognitive Coordinator, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-COG-REAS-F-R-01
Short title	Trust Functions Profiling and Storage
Description	Implement a reasoning engine that profiles trust functions and stores the related info based on past user interactions and system metrics to determine the level of trustworthiness.
AUR	Provide reliable trustworthiness assessments for system operations.

ID	REQ-COG-AISER-F-M-02
Short title	AI-Assisted Learning and Adaptation
Description	Integrate AI/ML algorithms for continuous learning and adaptation by maintaining and supporting CI/CD pipelines, to support code and training dataset revisions.
AUR	Maintain up-to-date level of trustworthiness provision and system adaptability.

ID	REQ-COG-AISER-F-M-03
Short title	AI Prediction Accuracy and Metrics

Description	Ensure that AI predictions achieve a high level of accuracy and compliance the KPIs such as MAE, MSE, R^2 etc
AUR	Provide more accurate results

ID	**REQ-COG-KBASE-F-M-04**
Short title	Advanced Knowledge Base That Supports The Reasoning Engine
Description	Develop an advanced knowledge base that stores relevant data, past decisions, user info and deployment actions by the TFs in order to assist the Reasoning Engine operations, resolve conflicts and proceed to deployments with maximum robustness
AUR	Ensure accurate and relevant data for the decision-making processes.

ID	**REQ-COG-REAS-F-R-05**
Short title	Context-aware Reasoning that supports Trust Score Calculation
Description	Develop context-aware reasoning capabilities by utilising the Knowledge Base to adapt decisions based on the situational context, user info and any conflicts that may arise in order to resolve them.
AUR	Improve decision relevance and accuracy.

ID	**REQ-COG-AISER-F-M-06**
Short title	Accurate Feature extraction
Description	Implement precise feature extraction mechanisms to accurately capture relevant data points from user inputs.
AUR	Provide more accurate results

ID	**REQ-COG-AISER-F-R-07**
Short title	Non-calibrated Output Validation
Description	Develop mechanisms to validate the non-calibrated outputs of the AI recommendation algorithm to ensure they meet accuracy standards.
AUR	Provide more accurate results

ID	**REQ-COG-AISER-F-M-08**
Short title	Explainable AI Models to Improve User's/Tenant's Level of Trust
Description	Integrate explainable AI models that provide transparency and justification for Cognitive Coordinator's decisions and the related system deployments.
AUR	Ensure users understand and trust AI-driven decisions through transparent explanations.

ID	**REQ-COG-KBASE-NF-R-09**
Short title	Ensure Knowledge Base Integrity

Description	Implement robust validation and change-management mechanisms to preserve the integrity, consistency and traceability of all data stored in the Knowledge Base, so that the Reasoning Engine operates only on verified, non-tampered and up-to-date information, thereby ensuring the accuracy, explainability and feasibility of its outcomes across all supported use cases.
AUR	User trust and system reliability

ID	**REQ-COG-SCHED-F-M-10**
Short title	Near-Real time data processing and response
Description	Integrate near-real time data processing and feature engineering for the seamless operation of the AI/ML models by utilising user info and system metrics.
AUR	Provide accurate results

ID	**REQ-COG-SCHED-F-M-11**
Short title	Management of Cloud Computing continuum resources
Description	The Cognitive Orchestrator must have the possibility to orchestrate and monitor the resources from the continuum infrastructure by utilising exposition to the related APIs.
AUR	N/A

ID	**REQ-COG-SCHED-F-M-12**
Short title	Service and Function Scheduling
Description	Develop a scheduling system that manages and optimizes the deployment of services and functions based on current network conditions and resource availability.
AUR	Optimize resource utilization and ensure timely service deployment.

ID	**REQ- COG -FRA-F-M-13**
Short title	Operational Processes Requirement
Description	The Cognitive Coordinator must be able to manage and monitor the operational processes of resilience functions, such as health checks. This could involve scheduling and executing health checks, logging results, and triggering alerts or actions based on those results.
AUR	N/A

ID	**REQ-COG -PRO-F-M-14**
Short title	Programmable Cognitive Coordination
Description	The Cognitive Coordinator must have a programmable framework that allows dynamic configuration and optimization of new AI models.
AUR	Ensure the cognitive coordinator can dynamically adapt to various operational scenarios.

5.4 Safety Function Requirements

5.4.1 Introduction

The development of the Safety Application Function that leverages the Software Defined Perimeter (SDP) paradigm, needs comprehensive and precise requirements to ensure robust security and optimal performance. This SDP-based function will safeguard the infrastructure nodes by creating individualized perimeters around network services, including various nodes, controllers, and data centres. By implementing fine-grained, user-centric micro-segmentation, the system restricts network exposure and mitigates potential attack vectors, granting users access only to the specific services they require.

The requirements reflect how the traditional SDP stack will be adapted to align with the SAFE-6G methodology while preserving its fundamental operating principles. This includes outlining the processes involved when a network user initiates access, triggering the SAFE-6G safety function to generate virtual SDP controller and initialize appropriate perimeters. These specifications will guide the development process, ensuring that each part functions cohesively to deliver a secure and efficient network experience tailored to individual user needs.

5.4.2 Safety Function Requirements

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the Safety Function component, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-FSAF-DES-F-M-01
Short title	SBA compatible design
Description	The Function must be designed in a compatible way to interact with the SBA of the core network.
AUR	N/A

ID	REQ-FSAF-DES-F-M-02
Short title	Interconnection with 5/6G Networks
Description	The Function must be interfaced with the NEF (CAPIF) function of the core network for pushing required policies regarding each UE.
AUR	N/A

ID	REQ-FSAF-COM-F-M-03
Short title	VPN technology
Description	The function must support a variety of VPN protocols, such as OpenVPN, WireGuard, IKEv2/IPsec, L2TP/IPsec, SSL
AUR	N/A

ID	REQ-FSAF-COM-F-M-04
Short title	SDP tunnel establishment

Description	The function must support the establishment of a tunnel between UE and the SDPGW using a VPN protocol (such as OpenVPN, WireGuard, IKEv2/IPsec, L2TP/IPsec, SSL).
AUR	N/A

ID	**REQ-FSAF-COM-F-M-05**
Short title	SDP tunnel UE authorization access
Description	The SDP tunnel must provide the UE with access to dedicated content and applications using the tunnel between UE and the SDPGW.
AUR	N/A

ID	**REQ-FSAF-COM-F-M-06**
Short title	Device & UE authentication
Description	The function must provide the proper authentication processes to authenticate device and user. The A4 server will store device and UE data along with requested target application of UE.
AUR	N/A

ID	**REQ-FSAF-DES-F-M-07**
Short title	Hosting Infrastructure - SBA
Description	The Function must be provisioned in an infrastructure following the SBA.
AUR	N/A

ID	**REQ-FSAF-DES-F-M-08**
Short title	Dynamic function creation
Description	The function must have the ability to communicate with MANO to mandate specific deployment actions for a specific session. The function will create a new control function along with a gateway (SDPCF & SDPGW) that will enforce specific policies to fulfil UE's requirement.
AUR	N/A

ID	**REQ-FSAF-COM-F-M-09**
Short title	Dynamic policies
Description	The function must offer dynamic policies triggered by events happening in the session. The AF will interact with MLops and will get the updated models to enforce dynamic policies across the network functions.
AUR	N/A

5.5 Security Function Requirements

5.5.1 Introduction

The security function provides a Distributed Ledger Infrastructure (DLT) for recording and storing executed audits, along with a Self-Sovereign Identity (SSI) approach that enables the use of verifiable credentials. The main objectives include securely storing audit results, implementing SSI in a zero-trust policy context, and supporting the tokenization of actions.

5.5.2 Security Function Requirements

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the Security Function, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-FSEC-NET-F-M-01
Short title	6G Component Interaction
Description	The function must be able to interact with various components of the 6G network, including the 6G core, MetaOS, and other relevant subsystems through the Common API Framework for 5G and beyond (CAPIF), to ensure smooth integration and data exchange across the network to employ the digital identity layer.
AUR	N/A

ID	REQ-FSEC-INT-F-M-02
Short title	Self-Sovereign Identity (SSI)
Description	The function should implement SSI in a zero-trust policy context, enabling the use of verifiable credentials to promote user autonomy, privacy, and decentralized secure identity verification.
AUR	N/A

ID	REQ-FSEC-COMP-NF-M-03
Short title	Smart Contract Security and Auditing
Description	The function must ensure that smart contracts used are finalized, secure, thoroughly tested, and free from vulnerabilities to prevent exploitation and maintain trust in the system. Additionally, the function should include a mechanism for regularly auditing smart contracts for compliance and security vulnerabilities, leveraging automated tools and manual reviews to ensure ongoing contract integrity.
AUR	N/A

ID	REQ-FSEC-COMP-NF-M-04
Short title	Comprehensive Audit Logging
Description	All actions taken by the function should be thoroughly logged and auditable, providing transparency and accountability essential for trust and compliance verification.

AUR	N/A

ID	**REQ-FSEC-INT-F-M-05**
Short title	Decentralized Identifiers (DIDs)
Description	The function should support the use of Decentralized Identifiers (DIDs) within the Aries framework to enhance privacy and security in identity management by allowing users to control their own identities. This includes the creation, usage, management and revocation of DIDs, as well as remote attestation to ensure the integrity and trustworthiness of the identifiers.
AUR	N/A

ID	**REQ-FSEC-COMP-F-M-06**
Short title	Secure Audit Storage
Description	The function focuses on providing a distributed ledger infrastructure, such as blockchain, for recording and storing executed audits, ensuring audit records are trustworthy, verifiable, and immutable.
AUR	N/A

ID	**REQ-FSEC-INT-F-M-07**
Short title	Tokenization through Verifiable Credentials (VCs)
Description	The function should implement SSI verifiable credentials to allow users to tokenize actions, audits and verification results of infrastructure components in a secure and transparent manner. User should be able to use these tokens to authorize invocations and provide authenticated proofs.
AUR	N/A

ID	**REQ-FSEC-COMP-NF-M-08**
Short title	Data Encryption
Description	The function must employ robust encryption methods for data at rest and in transit to protect sensitive information from unauthorized access and breaches.
AUR	N/A

ID	**REQ-FSEC-COMP-NF-M-09**
Short title	Identity Access Control Mechanisms
Description	The function must implement advanced access control mechanisms to ensure that only authorized users can access sensitive data and perform critical actions.
AUR	N/A

ID	REQ-FSEC-PER-F-M-10
Short title	Real-Time Security Processing
Description	The function should process identity verifications, audit logs, audit log backups and security policy updates in real-time to maintain network integrity and user security by providing timely responses to security events and access requests.
AUR	N/A

ID	REQ-FSEC-PER-NF-M-11
Short title	Scalable Security Handling
Description	The function must handle increasing numbers of users, devices, and transactions without impactful performance issues, supporting more extensive and complex identity operations as the 6G network grows.
AUR	N/A

ID	REQ-FSEC-PER-F-R-12
Short title	Customizable Security Policies
Description	The function should allow for customizable security policies and identity management rules based on a user centric approach to accommodate specific security needs.
AUR	N/A

ID	REQ-FSEC-PER-NF-M-13
Short title	High Reliability
Description	The function must provide consistent performance and with minimal downtime, ensure optimal performance, continuous security and trustworthiness across the network, while preventing single points of failure. Methods to achieve high reliability include load balancing, failover mechanisms etc.
AUR	N/A

ID	REQ-FSEC-PER-NF-M-14
Short title	Low-Latency Performance
Description	The function must operate efficiently with low latency to avoid bottlenecks in the network, ensuring that security processes do not impede network performance or user experience.
AUR	N/A

ID	REQ-FSEC-COMP-NF-M-15
Short title	Highest Security Standards
Description	The function must adhere to the highest security standards (OWASP, ISO/IEC, NIST, 3GPP SA3, IETF, W3C, etc.) to protect against breaches, unauthorized access, and data tampering, maintaining the integrity and trustworthiness of the 6G network.
AUR	N/A

ID	REQ-FSEC-INT-NF-R-16
Short title	Interoperability with Legacy Systems
Description	The function should ensure compatibility and interoperability with existing legacy systems, including older communication protocols and infrastructures such as 4G LTE, 5G networks, traditional network infrastructure and previous-generation security solutions. This facilitates a seamless transition and integration of new security measures.
AUR	N/A

5.6 Privacy Function Requirements

5.6.1 Introduction

The Privacy Function of the SAFE-6G framework ensures user data privacy and compliance with standards across 6G services. By leveraging AI-driven Decision Support Systems, it dynamically calculates and optimizes Privacy Scores in real-time. The function emphasizes interoperability, comprehensive auditing, and adherence to ethical guidelines to build user trust and transparency.

5.6.2 Privacy Function Requirements

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the Privacy Function, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-FPRI-PSC-F-M-01
Short title	Privacy Score Calculation Algorithm
Description	The function must implement a robust algorithm to calculate the PS, considering a variety of factors such as user data sensitivity, service provider's privacy policy, and current network security conditions.
AUR	N/A

ID	REQ-FPRI-DSS-F-M-02
Short title	Modular AI DSS Architecture
Description	The AI Decision Support System (DSS) must be designed with a modular architecture, facilitating easy updates and integration of new algorithms and models, supporting both rule-based and machine learning models interchangeably.
AUR	N/A

ID	REQ-FPRI-GEN-F-M-03
Short title	Comprehensive Logging and Auditing
Description	The function must implement comprehensive logging and auditing mechanisms to document all decisions made by the DSS and the data utilized, ensuring secure storage and easy retrieval for compliance and analysis.
AUR	N/A

ID	REQ-FPRI-GEN-NF-M-04
Short title	Service Provider Privacy Information Integration
Description	The function must establish a standardized structure for service providers to submit information regarding their privacy preservation methods through their interaction with the chatbot.
AUR	N/A

ID	REQ-FPRI-GEN-F-M-05
Short title	Integration with MetaOS for Metrics Retrieval
Description	The privacy function must be able to access MetaOS to retrieve essential metrics that influence privacy management, such as user density, data traffic, and service usage patterns, to enhance the accuracy and relevance of privacy assessments.
AUR	N/A

ID	REQ-FPRI-GEN-F-M-06
Short title	Interface with SAFE-6G Cognitive Framework
Description	The privacy function must interface seamlessly with the SAFE-6G cognitive framework, enabling dynamic adaptation to privacy threats and operational demands.
AUR	N/A

ID	REQ-FPRI-GEN-F-M-07
Short title	MLOps Integration for ML Lifecycle Management
Description	The function must offload machine learning lifecycle management tasks to the MLOps component to ensure efficient scaling, deployment, and maintenance of AI-driven privacy models.
AUR	N/A

ID	REQ-FPRI-PSC-F-M-08
Short title	Near Real-Time Privacy Score Assessment
Description	The privacy function must include a near real-time monitoring system that continuously assesses and updates the Privacy Score (PS) based on current network conditions and service details.
AUR	N/A

ID	REQ-FPRI-DSS-F-M-09
Short title	Scalability and Performance Optimization
Description	The DSS architecture must be horizontally scalable to manage increasing data volumes and user requests efficiently, with optimized performance to handle high-load conditions.
AUR	N/A

ID	REQ-FPRI-GEN-NF-M-10
Short title	Fault Tolerance and Data Access Redundancy
Description	The system must include robust fault tolerance mechanisms to maintain functionality and access to real-time data even in the event of partial system failures or external disruptions.
AUR	N/A

5.7 Resilience Function Requirements

5.7.1 Introduction

Resilience function is a SAFE-6G framework component which handles all network resource-related functionalities to bring up every user-centric 5G/6G customized mobile network. It is composed by per-user AI intelligence able to evolve user-centric instances as per user requirements during execution and handles the whole lifecycle of the instances.

5.7.2 Resilience Function Requirements

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the Resilience Function, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-FRES-FRA-F-M-01
Short title	SAFE-6G framework enrolment and dynamic function configuration endpoints.
Description	The Resilience function should be able to interact with the SAFE-6G framework to consume and get information about the trustworthiness level of core network, deployment location, resource availability of Resilience function, storage of resilience data to be consumed and operational processes of resilience function (e.g., health checks) via REST API.
AUR	N/A
Priority	M

ID	REQ-FRES-FRA-F-M-02
Short title	Trustworthiness Level API Requirement
Description	The Resilience function must include a method to consume the trustworthiness level from the SAFE-6G framework. This method should support standard HTTP protocols and be compatible with processing information returned in formats such as JSON.
AUR	N/A
Priority	R

ID	REQ-FRES-DATA-F-M-03
Short title	User Intent Requirement
Description	The Resilience function must be able to accept specific user intents and semantics provided via the chatbot. These intents should be processed and acted upon to improve network resilience.

AUR	N/A
Priority	M

ID	**REQ-FRES-DATA-F-M-04**
Short title	Resilience Action Requirement
Description	The system must be able to take resilience actions based on the insights gained from the MLOps framework. These actions should aim to enhance the robustness, fault-tolerance of the network, and scaling resources.
AUR	N/A
Priority	M

ID	**REQ-FRES-NET-F-M-05**
Short title	Core 5G/6G resilience customization through APIs
Description	The resilience function will configure on-demand core function USN nodes. To that end, it should be able to manage the APIs exposed by NEF to operate redundancy over AMF, UPF, SMF services.
AUR	N/A
Priority	M

ID	**REQ-FRES-FRA-F-M-06**
Short title	Resilience Function Information API Requirement
Description	Resilience function must have access to an API endpoint that returns deployment, location, and resource availability information of the Resilience function. This endpoint should also support standard HTTP methods and return data in a commonly used format.
AUR	N/A
Priority	R

ID	**REQ-FRES-INFRA-F-M-07**
Short title	Redundancy Requirement
Description	The resilience function should implement redundancy within the MetaOS infrastructure. This could involve duplicating critical components or functions to increase reliability and availability.
AUR	N/A
Priority	R

ID	**REQ-FRES-NET-NF-M-08**
Short title	Security Requirement
Description	All interactions between the Resilience function and other SAFE-6G components via CAPIF must be secure. This includes data encryption, authentication, and authorization.
AUR	N/A

Priority	O

ID	REQ-FRES-NET-NF-M-09
Short title	Resilience Function API Integration Requirement
Description	The Resilience function must interact with the OpenCAPIF to expose and consume the APIs following the implementation of ETSI SDG.
AUR	N/A
Priority	R

ID	REQ-FRES-NET-F-M-10
Short title	Customization Requirement
Description	The resilience function must allow for the customization of core 5G/6G resilience through APIs. This could involve adjusting parameters, enabling or disabling features, or other forms of customization.
AUR	N/A
Priority	R

ID	REQ-FRES-INFRA-F-M-11
Short title	Resilience Mechanisms to Manage Infrastructure via REST APIs and GitOps
Description	From REST APIs GitOps, the resilience function will modify the Core Network Functions descriptors to implement HA (High Availability) and redundancy on the MetaOS infrastructure through cloud continuum methods.
AUR	The SAFE-6G user will provide via user intents the requirements to have a level of resilience which will entail certain level of redundancy within the infrastructure.
Priority	R

ID	REQ-FRES-NET-F-M-12
Short title	On-Demand Configuration Requirement
Description	The resilience function must be able to configure core function USN nodes on-demand. This should be done in a way that minimizes disruption to the network and ensures optimal performance.
AUR	N/A
Priority	R

ID	REQ-FRES-NET-NF-M-13
Short title	Performance Monitoring Requirement
Description	The resilience function must monitor the performance of the core function USN nodes and the redundant AMF, UPF, SMF functions. This could involve tracking metrics, generating reports, and triggering alerts or actions based on performance data.
AUR	N/A
Priority	R

5.8 Reliability Function Requirements

5.8.1 Introduction

The user-centric reliability function will first collect data from all virtual, computational and network resources and deliver them to the local model training module. Then, the local model training module (i.e., AI-agent of SAFE-6G Cognitive Coordinator) will be fed by the data provided by the multi-layer monitoring system which profiles the service and the infrastructure for different operational conditions. Next, these collected input-output data pairs will train ML methods locally on the client side, which will be able to perform predictions on the target performance metrics for different operational conditions.

Second, all this intelligence will lead to making optimal decisions for the applicability of the necessary configurations and policies for the provision of reliability, as per the user's request. For example, to avoid approaching potential system breaking points, such as reaching the maximum utilization of virtual or physical resources. Further, during the reliability profiling, the deployed service and the pre-trained ML/AI methods will be employed to perform inspection for abnormalities or malicious actions.

Finally, the data collected from the multi-layer mechanism will be stored, and a report will be exported to evaluate the overall performance of the reliability function.

5.8.2 Reliability Function Requirements

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the Reliability Function, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-FREL-NET-F-M-01
Short title	Interface to communicate with the cognitive SAFE-6G coordination component
Description	The communication between the Reliability function and the cognitive SAFE-6G coordination component is required to send the generated events.
AUR	N/A

ID	REQ-FREL-AI-NF-M-02
Short title	Training of reliability AI models
Description	The reliability function will train AI models to perform predictions about the avoidance of potential service breaking points and identification of security threats.
AUR	N/A

ID	REQ-FREL-AI-NF-M-03
Short title	Model selection per level of trustworthiness
Description	The Reliability function must be able to choose between different ML models, according to the selected level of trustworthiness.
AUR	N/A

ID	REQ-FREL-RES-NF-O-04
Short title	Provision of HPC infrastructure for training of ML models
Description	The ML methods based on the specific details of the task that is to be solved, e.g., number of input features, number of samples, can be of very high complexity. For this reason, they may require acceleration of the training and inference processes via HPC to reduce these times.
AUR	N/A

ID	REQ-FREL-RES-NF-M-05
Short title	Function interoperability
Description	The reliability function must be able to consume streaming monitoring data from the monitoring system related to the infrastructure and user service status.
AUR	N/A

ID	REQ-FREL-NET-F-R-06
Short title	Restrict unauthorized access
Description	Reliability function should be executed in a secure environment not accessible by public networks.
AUR	N/A

ID	REQ-FREL-NET-NF-R-07
Short title	Evaluation report
Description	The Reliability function at the post-deployment phase must communicate with the MLOps, which will create the evaluation report, including the various metrics, e.g., attainable accuracy, training time, inference time, etc.
AUR	N/A

5.9 MLOPs Requirements

5.9.1 Introduction

SAFE-6G introduces the MLOPs Framework concept which, in a nutshell, covers the whole lifecycle of the distributed AI/ML models, including AI/ML model creation and orchestration. Being infrastructure agnostic, the MLOPs is capable of in-network training AI/ML models and, supported by the XAI module, exposing users/tenants a sort of human-like rational explanation about the LoT provided by the cognitive coordinator layer.

The datasets to produce the AI/ML models come from the monitoring modules, which aggregate the data from the continuum. In addition, a DT component complements the dataset where neither there is real-data available from the 6G infrastructure nor real data is enough to properly complete the training process. The datasets for training AI/ML models could contain sensitive information from data owners and, therefore, the models should not expose any private and sensitive information during the training. To this end, a Differential Privacy (DP) module, which is a perturbation mechanism, is

implemented to add some noise or randomness to the datasets without, however, affecting the models' accuracy.

5.9.1.1 MLOPs PRESENTATION

The MLOPs framework consists of several modules to cope with the necessity of the project in terms of providing intelligence to the different layers of the architecture. In such sense, the MLOPs framework offers the following modules:

- Pipeline development
- Pipeline orchestration platform (POP)
- Trained AI/ML models
- Model serving
- Inference
- Differential privacy
- Perturbated datasets
- Digital twin
- XAI

These components are presented in detail in later deliverables (i.e., Deliverable D2.2 Overall SAFE-6G Framework and Reference Architecture Design).

5.9.2 MLOPs REQUIREMENTS

The requirements outlined in the common requirements list in Section 5.1.2 are also applicable to the MLOPs component, but further extended hereby with additional requirements that are specific and applicable only to this SAFE-6G component:

ID	REQ-MLOPS-XAI-F-M-01
Short title	Collect inputs for XAI component
Description	Inputs for the XAI component take the form of the model results coming from the five trustworthiness functions. The result to be explained may take the form of: • A particular value to be analysed (i.e., an anomaly returned by the model), • The global behaviour of the model (i.e., how the model splits low values against high values). The inputs for the XAI component will concern results function by function (correlations between functions will not be considered).
AUR	N/A

ID	REQ-MLOPS-TRAIN-F-M-02
Short title	Collect data for training
Description	For training purposes, it is need it representative datasets to provide a meaningful ML model.
AUR	N/A

ID	REQ-MLOPS-DEV-F-M-03
Short title	AI/ML model and dataset provided by the user
Description	During the pipeline development step, the user must provide an AI/ML model to be trained along with a dataset.
AUR	N/A

ID	REQ-MLOPS-XAI-F-M-04
Short title	Build XAI models
Description	The XAI component proposes two kinds of models to explain results of the five trustworthiness functions AI model: • Local explanation models to explain a particular value (anomalies, outliers) returned by the five trustworthiness function model results, • Global explanation results to understand the global behaviour of these models.
AUR	N/A

ID	REQ-MLOPS-XAI-F-M-05
Short title	Send results to the chatbot
Description	The results obtained by the XAI component will be integrated into the chatbot so that XAI results will be communicated to the end-users.
AUR	XAI results will help end-users to better understand the results of the five trustworthiness functions AI models.

ID	REQ-MLOPS-XAI-F-M-06
Short title	Propose different visualizations of the XAI results
Description	Explainable results will take the form of text, numbers, tables, graphs, scatter plots or other visualizations.
AUR	XAI results will help the end-users to better understand the results of the five trustworthiness functions AI models

ID	REQ-MLOPS-INF-F-M-07
Short title	Inference connectivity
Description	The inference module must have connectivity with the cognitive layer to inference the module to the function owners getting a result to make decisions.
AUR	N/A

ID	REQ-MLOPS-XAI-NF-M-08
Short title	The XAI component should allow real-time interactions with the end-user
Description	Real time interactions with the end-user (thanks to the chatbot) should be possible so that end-users may interact with the XAI results.

AUR	The system should allow quick interactions with the end users to facilitate the understanding of the XAI results.

ID	REQ-MLOPS-TRAIN-F-R-09
Short title	Anonymization of datasets
Description	Datasets must be anonymized previous to the training phase so no sensitive data can be consumed.
AUR	N/A

ID	REQ-MLOPS-MLLIB-F-M-10
Short title	Large database to store ML models
Description	The database in the platform must be big enough to store all the ML models generated by the Function owners, as well as connectivity with POP and the serving model module.
AUR	N/A

ID	REQ-MLOPS-DT-NF-R-11
Short title	Digital Twin (DT) providing accurate and sufficient data
Description	When DT is required to simulate possible scenarios, the data generated from the DT must be as accurate as possible to real data as well as enough to train the models.
AUR	N/A

ID	REQ-MLOPS-DP-NF-M-12
Short title	Accuracy in datasets regardless the level of noise introduced by Differential privacy
Description	Differential privacy adding noise to dataset must provide a high accuracy to provide a meaningful ML model.
AUR	N/A

5.10 User Centric Distributed 6G Core Requirements

5.10.1 Introduction

The 6G core should follow the SBA paradigm extended with user centric functionality. This requires that each NF when registered to the Network Repository Function (NRF) should include additional information to differentiate the user specific functions.

5.10.2 User Centric Distributed 6G Core Requirements

ID	REQ-UCEN-DES-F-M-01
Short title	User centric functionality description
Description	The user centric 5G/6G core functions should include additional service type or service description information which will be used to differentiate user functions when searching in the NRF.

AUR	N/A

ID	REQ-UCEN-DES-F-M-02
Short title	Standalone NF
Description	The user centric network function should be designed as standalone without dependencies from other NF so they can be instantiated on need basis. When required the standalone user centric NF is launched, registered to NRF with sufficient information to be discoverable from NRF by the consumer NF.
AUR	N/A

ID	REQ-UCEN-DES-F-R-03
Short title	Each NF should be containerized
Description	Each function of the core network (USN, NSN/Trust function) should be individually containerized.
AUR	N/A

ID	REQ-UCEN- DES-F-R-04
Short title	Core network shall be able to support auxiliary NFs
Description	Core network shall be able to support auxiliary copies of the NFs in order to be capable of realising resilient and trustworthy scenarios tailored to the trustworthiness level that the SAFE-6G system mandates.
AUR	N/A

ID	REQ-UCEN-COMP-F-M-05
Short title	Core network exposure must be performed via the OpenCAPIF
Description	Core network will implement the CAPIF SA6 specification following the OpenCAPIF implementation of ETSI SDG.
AUR	N/A

ID	REQ-UCEN-COMP-F-M-06
Short title	The core network must comply with the 3GPP Standardization
Description	Any advancement made in the core network design must be compliant to the 3GPP standardization.
AUR	N/A

ID	REQ-UCEN-COMP-F-M-07
Short title	Core network functions and Trust function interaction must comply with SA6 3GPP specifications
Description	USN/NSN and Trust functions are envisaged as functions of the core network, but the trust functions are not currently a standardised addition to the core network,

	so they will be treated as vertical applications and their interaction with the core will follow the 3GPP SA6 paradigm.
AUR	N/A

5.11 Edge-Cloud Continuum Infrastructure Requirements

5.11.1 Introduction

The cloud continuum in 6G will allow the realisation of the USN and NSN services in a distributed and adapted way closer to users, tenants, applications, data sources, and regulated processes. Another key benefit of the envisioned user-centric redesign of the distributed 6G core architecture is the ease with which new services can be created, placed, subsequently scaled and moved between the clouds of the continuum (i.e. far edge, near edge, central cloud on which the 6G core is realised), and the efficiency with which they can be executed.

The cloud-native paradigm over the edge-cloud continuum will be followed for the whole design and development of the whole SAFE-6G framework components and the user-centric distributed 5G/6G core network over the edge cloud continuum. Moreover, compatibility with currently developing edge-cloud continuum MetaOS, such as the one of aerOS Horizon Europe project, will be pursued, reassuring interoperability, compatibility and sustainability of the proposed SAFE-6G framework in future deployments.

5.11.2 Edge-Cloud Continuum Infrastructure Requirements

ID	REQ-INFRA-RES-NF-M-01
Short title	Distributed, dynamic and heterogeneous ecosystem of computing resources
Description	Computing (i.e., CPU, GPU, RAM) and storage resources can be available anywhere in the network (edge, fog, cloud), defining an expanded network compute fabric that can be leveraged by the SAFE-6G framework (6G core, chatbot, MLOPs module, and trust functions), as well as the vertical applications related to the use cases. These resources can vary over time, in different geo-distributed locations, with resources added or deleted over time.
AUR	N/A

ID	REQ-INFRA-RES-NF-M-02
Short title	Support of Cloud Native technologies
Description	The underlying infrastructure must support containerization and container orchestration technologies (mainly Docker/containerized and Kubernetes), as the SAFE-6G framework will work following the Cloud Native paradigm.
AUR	N/A

ID	REQ-INFRA-META-NF-M-03
Short title	Meta-operating system for the IoT edge-cloud continuum
Description	A meta-operating system for the distributed computing continuum will be deployed on the Infrastructure Elements, owned by one or different tenants, with the main

	objective of (smartly) orchestrating, connecting and monitoring services and applications over them. As the project will follow the Cloud Native paradigm, the MetaOS will include *de facto* standards/technologies, such as Prometheus, on its proposed stack.
AUR	N/A

ID	**REQ-INFRA-META-NF-M-04**
Short title	Exposure capabilities of the meta-operating system
Description	The meta-operating system will expose a set of interfaces (Open APIs) to facilitate the communication between Infrastructure Elements, the access to monitoring and analytic data, and its management of the MetaOS system itself. Graphical user interfaces will be available to support the latter. If additional metrics are required by other modules of the SAFE-6G framework, dedicated monitoring agents/export will be integrated (existing or specifically created).
AUR	N/A

ID	**REQ-INFRA-META-NF-M-05**
Short title	Data accessibility across the computing continuum
Description	Data gathered from heterogeneous sources should be accessible from any place of the continuum, considering access rights. As described in the previous requirement, these data can be related to the use cases, the SAFE-6G framework, and the meta-operating system itself.
AUR	N/A

ID	**REQ-INFRA-RES-NF-M-06**
Short title	Infrastructure availability and resiliency
Description	The infrastructure should have enough resources for supporting the framework and the use cases, with dedicated self-scaling mechanisms to allocate the needed resources for the hosted services (related to both SAFE-6G platform and use cases). The system should also adapt to unexpected or abrupt changes in the network, so services can keep working without significant disruption, ensuring Quality of Service (QoS) and end Quality of Experience (QoE).
AUR	N/A

ID	**REQ-INFRA-NET-NF-M-07**
Short title	Real-time communications
Description	5G/6G must be part of the access networks available at the continuum, to provide low-latency, real-time communication capabilities to support the use cases of the project. Specific requirements in terms of e.g., bandwidth, latency or jitter will be provided by their developers.
AUR	N/A

ID	REQ-INFRA-NET-NF-M-08
Short title	Service visibility
Description	All services must be reachable among them regardless of their positioning within the managed computing continuum, unless prevented by network policies due to trustworthy or security reasons (e.g., a very restrictive policy may deny all traffic by default, having specific ones for allowing some types of traffic).
AUR	N/A

ID	REQ-INFRA-NET-NF-M-09
Short title	Reallocation capabilities for ensuring low latency requirements
Description	System latency must be monitored to ensure that the demands of use cases are met, enabling the possibility of reallocating the services if their requirements are not met.
AUR	N/A

ID	REQ-INFRA-NET-NF-M-10
Short title	Secure network connectivity
Description	Communications must be secured via virtual private networks and data encryption features, to protect critical data travelling through the managed computing continuum.
AUR	N/A

ID	REQ-INFRA-SEC-NF-M-11
Short title	Management of identity and access to the meta-operating system
Description	The system must incorporate authentication, authorization and user management components to ensure that only registered users/services with the proper rights can access the features provided by the MetaOS, exposed to the outside via (secured) Open API.
AUR	Tenants need to have granted access to the cloud continuum infrastructure prior to the deployment of the user-centric infrastructure.

ID	REQ-INFRA-NET-NF-R-12
Short title	Load balancing adapted to 6G needs
Description	The meta-operating system must include a load balancer adapted to the requirements of the 5G/6G core interfaces, according to the Service Communication Proxy (SCP) specifications of 3GPP release 16.
AUR	N/A

ID	REQ-INFRA-NET-NF-O-13
Short title	Service function chaining capabilities

Description	The meta-operating system should support Service Function Chaining (SFC) capabilities for some specific network-related services. Specifically, chaining of functions for incoming traffic (to go through, e.g., firewall, NAT, load balancer).
AUR	N/A

6 Conclusion And Next Steps

This deliverable describes the first ideas to build the SAFE-6G platform, in terms of the definition of a blueprint architecture, the identification of stakeholders and actors who will use or benefit from such a platform. Based on this analysis, a list of key requirements associated to SAFE-6G framework has been proposed. Lastly, two use cases have been defined to test and guarantee the viability of the SAFE-6G platform.

The blueprint architecture highlights the importance, in the envisioned 6G ecosystem, of trusted connections that are critical for all parties involved, extending security and privacy to a more inclusive framework, such as trustworthiness, which should be assured as a native feature. The document clarifies the term "trustworthiness", at the heart of the project, which refers to a holistic approach, including safety, security, privacy, resilience, and reliability. SAFE-6G aims at implementing such a trustworthy framework to support and enhance the trust over the next evolution of the 5G network and the managed resources.

The deployment of this new architecture is expected to introduce several modifications in the current identification of stakeholders and their roles. From the rich list of identified of current or potential stakeholders and actors who will benefit from the use of SAFE-6G platform, specific concerns are described, with the stakeholders they involved and their roles for each of them.

From this analysis, an extended set of requirements has been presented aspiring to influence technical designs with the most ambitious challenges for breakthrough designs. The proposed architecture allowed the definition of domains on which technical requirements have been defined. Nine domains have been defined and cover: user-centric distributed 6G core, cognitive coordinator, five SAFE-6G functions (Safety, Security, Privacy, Resilience, Reliability), MLOPs, Edge-Cloud continuum plane.

Finally, the first definition of the two use-cases was used to extract an initial set of insights and challenges from a trustworthiness perspective. A first analysis shows that the two use cases cover the five functions in terms of trustworthiness needs.

The next iterations among the technical teams in *WP2- Realisation Process, Requirements and Reference Architecture Design* are expected to more accurately and realistically target the envisaged functionality and if needed prioritize the requirements in the most viable way. The results will be refined in deliverables *D2.2- Overall SAFE-6G Framework and Reference Architecture Design* (due in M10/October 2024) and *D2.3- Metaverse use-cases definition with virtual-assistant for user-centric configuration* (due in M12/December 2024).

7 REFERENCES

[1] ISO Central Secretary, “Systems and software engineering – Systems and software quality requirements and evaluation (SQuaRE) – Measurement of quality in use,” International Organization for Standardization, Standard ISO/IEC 25022, 2016. [Online]. Available: https://www.iso.org/standard/35746.html

[2] L. Kastner, et al., "On the Relation of Trust and Explainability: Why to Engineer for Trustworthiness," in 2021 IEEE 29th International Requirements Engineering Conference Workshops (REW), Notre Dame, IN, USA, 2021 pp. 169-175. doi: 10.1109/REW53955.2021.00031

[3] X. Yan, X. An, W. Ye, M. Zhao, Y. Xi and J. Wu, "User-Centric Network Architecture Design for 6G Mobile Communication Systems," 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023, pp. 305-310, doi: 10.1109/EuCNC/6GSummit58263.2023.10188283.

[4] L. Chazette, W. Brunotte, and T. Speith, “Exploring explainability: A definition, a model, and a knowledge catalogue,” in IEEE 29th International Requirements Engineering Conference (RE). IEEE, 2021.

[5] W. Pieters, “Explanation and trust: What to tell the user in security and AI?” Ethics and Information Technology, vol. 13, no. 1, pp. 53–64, 2011.

[6] R. Guidotti, A. Monreale, S. Ruggieri, F. Turini, F. Giannotti, and D. Pedreschi, “A survey of methods for explaining black box models,” ACM Computing Surveys, vol. 51, no. 5, pp. 1–42, 2019.

[7] M. T. Ribeiro, S. Singh, and C. Guestrin, “‘Why Should I Trust You?’: Explaining the predictions of any classifier,” in Proceedings of the 22nd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining. New York, NY, USA: Association for Computing Machinery, 2016, pp. 1135–1144.

[8] M. Langer, D. Oster, T. Speith, H. Hermanns, L. Kastner, E. Schmidt, A. Sesing, and K. Baum, “What do we want from explainable artificial intelligence (XAI)? – A stakeholder perspective on XAI and a conceptual model guiding interdisciplinary XAI research,” Articifial Intelligence, vol. 296, 2021.

[9] Ethics Guidelines for Trustworthy Artificial Intelligence, available online at https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

[10] X. Yan, X. An, W. Ye, M. Zhao, Y. Xi and J. Wu, "User-Centric Network Architecture Design for 6G Mobile Communication Systems," in 2023 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Gothenburg, Sweden, 2023.

[11] C. Li, W. Hua, A. Ming y S. Shaohui, «AI-native User-Centric Network for 6G,» 2022 IEEE/CIC International Conference on Communications in China (ICCC Workshops), nº 10.1109/ICCCWorkshops55477.2022.9896699, pp. 494-499, 2022.

[12] S. Chen, L. Chen, B. Hu, S. Sun, Y. Wang, H. Wang and W. Gao, "User-Centric Access Network (UCAN) for 6G: Motivation, Concept, Challenges and Key Technologies," IEEE Network, vol. 38, no. 3, pp. 154-162, 2024.

[13] IEEE standard 1471

[14] ISO/IEC 25010 available online at https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-2:v1:en

[15] ISO/IEC 25000 available online at https://iso25000.com/index.php/en/iso-25000-standards/iso-25010

[16] N. Gkatzios, H. Koumaras, D. Fragkos and V. Koumaras, "A Proof of Concept Implementation of an AI-assisted User-Centric 6G Network," 2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Antwerp, Belgium, 2024, pp. 907-912, doi: 10.1109/EuCNC/6GSummit60053.2024.10597020.

[17] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels,” RFC 2119, BCP 14, Mar. 1997.