6GSNS

Co-funded by the European Union

SAFE-6G

SAFE-6G

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

Deliverable D2.3: Metaverse use-cases definition with virtual assistant for user-centric configuration

Date: 18/12/2025

Version: v1.1

DISCLAIMER

Grant Agreement	101139031
Document number	D2.3
Document title	Metaverse use-cases definition with virtual assistant for user-centric configuration
Lead Beneficiary	IMM
Editor(s)	Charles Bailly (IMM)
Author(s)	Charles Bailly (IMM) Javier Garcia (TID) Vasiliki Rentoula (NCSRD) Harilaos Koumaras (NCSRD) Spyridon Georgoulas (NCSRD) Ilias Alexandropoulos (NCSRD) Panagiotis Karkazis (UNIWA) Dimitris Uzunidis (UNIWA) Stamatia Drampalou (UNIWA) Zouzias Dimitris (eBOS) Constantinos Fragkos (INF) Vaios Koumaras (INF) Nikolaos Zombakis (8BELLS) Guillaume Hébert (KEY) Van Hoan Hoang (KEY)
Dissemination level	Public
Contractual date of delivery	31/12/2024
Status	Final
File name	SAFE-6G_D2.3_V1.1.pdf

Revision History

Version	
V0.1	Table of Contents and expected content per Section.
V0.2	Initial Contribution by all partners.
V0.3	Second round of contributions by all partners.
V0.4	First revision and homogenization of the content conducted by TID, NCSRD and UNIWA.
V0.5	Version produced by IMM based on the comments from the First Review.
V0.6	Additional input in Use-case KVIs section.
V0.8	Second Review performed by the Technical Steering Committee.
V0.9	Final draft and homogenization of content produced by IMM based on the comments from the Second Review. Final review performed by the Project Coordinator and the Editor.
V1.0	Final version following the Quality check
V1.1	Updated version after mid-term review

GLOSSARY

Abbreviations/Acronym	Description
AI	Artificial Intelligence
API	Application Programming Interface
AR	Augmented Reality
B5G	Beyond 5G
cLoT	calibrated Level of Trustworthiness
DP	Differential Privacy
DT	Digital Twin
EC	European Commission
HMD	Head-Mounted Display
JWT	JSON Web Tokens
LoTw	Level of Trustworthiness
N/A	Not available
NF	Network Function
nLoT	non-calibrated Level of Trustworthiness
QoE	Quality of Experience
QoS	Quality of Service
RPCs	Remote Procedure Calls
TF	Trust Functions
TLS	Transport Layer Security
UC1	Use-Case 1
UC2	Use-Case 2
USD	Universal Scene Description
VR	Virtual Reality
XAI	eXplainable AI
XR	Extended Reality

EXECUTIVE SUMMARY

Use-cases are essential for guiding the design of the next generation of networks and align the concrete needs of end-users. This is especially true for SAFE-6G, which aims at designing a user-centric approach for 6G network to increase the trust users have in them. Beyond performance levels and security features, the goal of SAFE-6G is thus to implement such trustworthy 6G ecosystem and validate that this approach can bring a real added value for end-users. To do so, two metaverse use-cases had been selected to highlight the benefits of SAFE-6G: 1) an Industry 4.0 use-case based on Extended Reality (XR) applications for a factory Digital Twin (DT) and 2) an Education/Formation use-case based on XR+AI.

The present document details these two use-cases. It showcases the result of the last refinement iteration of the two use-cases, the involved stakeholders and the benefits offered by SAFE-6G for them. Then, the document introduces the requirements, KPIs and KVIs emerging from the use-case scenarios, *i.e.* the expectations coming from the perspective of end-users. Finally, the technical architecture designed for each use-case is detailed to serve as reference for the incoming implementation tasks of the project.

This document is the third deliverable of WP2. It completes two previous deliverables: *D2.1 - Definition of Technical Requirements for User-centric 6G Trustworthiness* and *D2.2 - Overall SAFE-6G Framework and Reference Architecture Design.*

KEYWORDS

6G, Trustworthiness, Use-cases, User requirements, XR

TABLE OF CONTENTS

List of FIGURES

List of TABLES

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. This deliverable describes in detail the two use-cases selected to highlight the benefits of the SAFE-6G approach. It presents the scenarios, needs and expectations for the SAFE-6G system from the end-users' perspective.

1.2 STRUCTURE OF THE DOCUMENT

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

- Chapter 2 extends the initial SAFE-6G metaverse use-case descriptions provided in D2.1, detailing their respective scenarios, stakeholders and benefits offered by SAFE-6G.
- Chapter 3 presents the list of requirements, KPIs and KVIs emerging from the two use-cases.
- Chapter 4 details the technical architectures designed from the elements presented in previous chapters. It presents the explored technical solutions, and the final architecture selected for the metaverse applications and their connection to SAFE-6G components.
- The Conclusion and Next Steps Section gives a summary of the work performed and the next incoming 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 use-cases, the identified end-users' requirements and KPIs in addition to the presented technical architectures will contribute to the adoption of SAFE-6G approach for building a trustworthy and user-centric 6G system.

2 SAFE-6G METAVERSE USE-CASES

2.1 USE-CASE 1: FACTORY DIGITAL TWIN

2.1.1 USE-CASE 1 SCENARIO

As presented in D2.1, Use-Case 1 (UC1) is built around the Digital Twin (DT) of a factory with several production lines. When a mechanical or organizational problem is detected in a production line, the DT notifies two managers who will collaborate in Extended Reality (XR) to define an appropriate solution and trigger the corresponding changes into the DT. These changes will later be reflected in the real factory under the supervision of technicians.

The second iteration of UC1 introduced one major refinement: the separation of manager users into two distinct profiles. The first identified profile is: 1) the *Production Director*. Production directors oversee the production at the factory level. They thus have a global view of all production lines. On the contrary, 2) *Production Line Managers* are dedicated to a single production line. They thus are more specialized, with limited accreditation levels on the rest of the factory.

Distinguishing these two roles has significant implications for UC1 in terms of trustworthiness features. It introduces asymmetry between the metaverse application end-users, who still need to collaborate efficiently in XR despite not having the same features and authorizations in the factory DT.

These new aspects are reflected in the following Figures, which represent the detailed steps of the scenario of UC1.

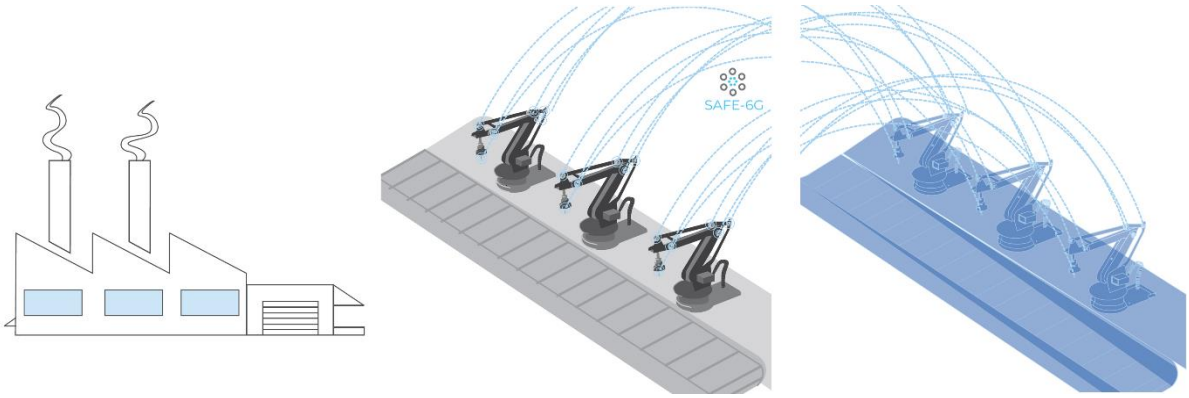

Figure 1: An Industry 4.0 factory has a digital twin of its production lines.

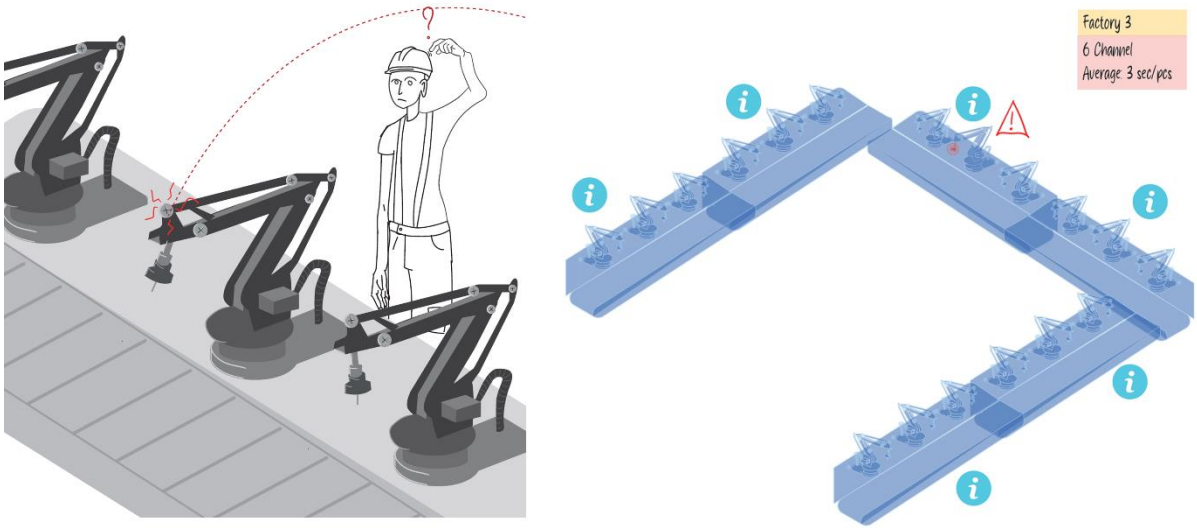

Figure 2: When an issue is detected on the production line, it is reflected on its digital replica. An adaptation may be required on the production line to limit risks and downtimes.

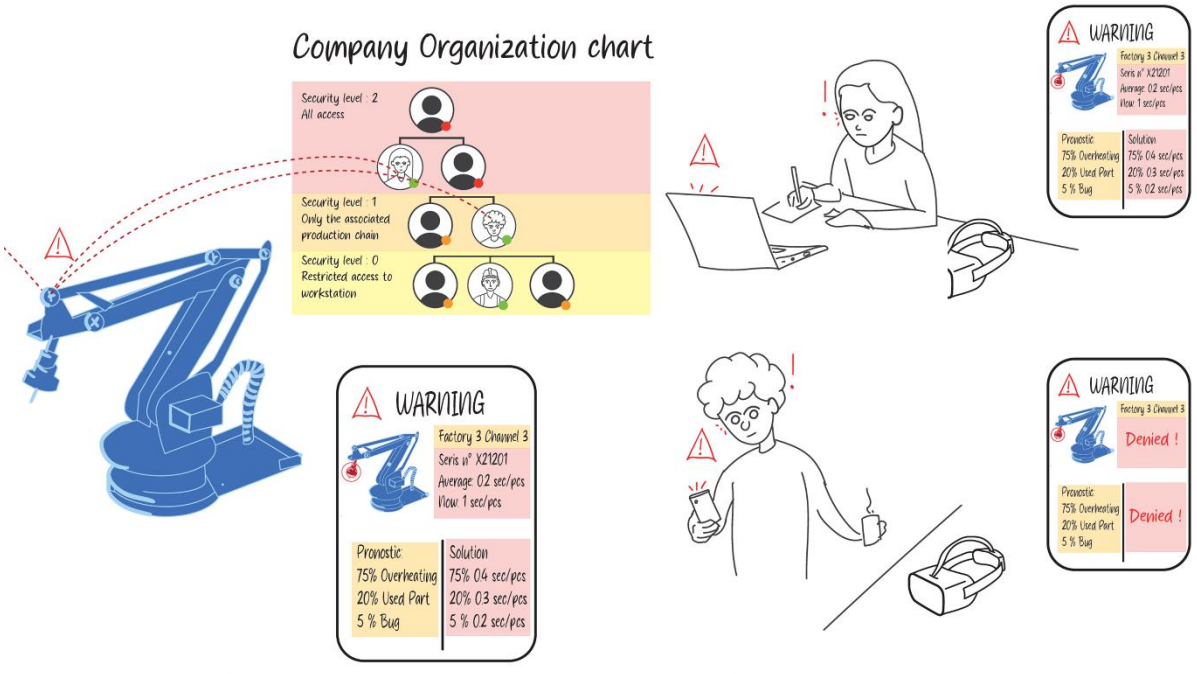

Figure 3: A production director and a line manager are notified. They have different accreditations and thus different access levels.

Figure 4: Users both connect their XR headsets to the SAFE-6G network and then authenticate themselves on the metaverse application. Removing the headset at any time locks the metaverse application. The user will need to be re-authenticated each time.

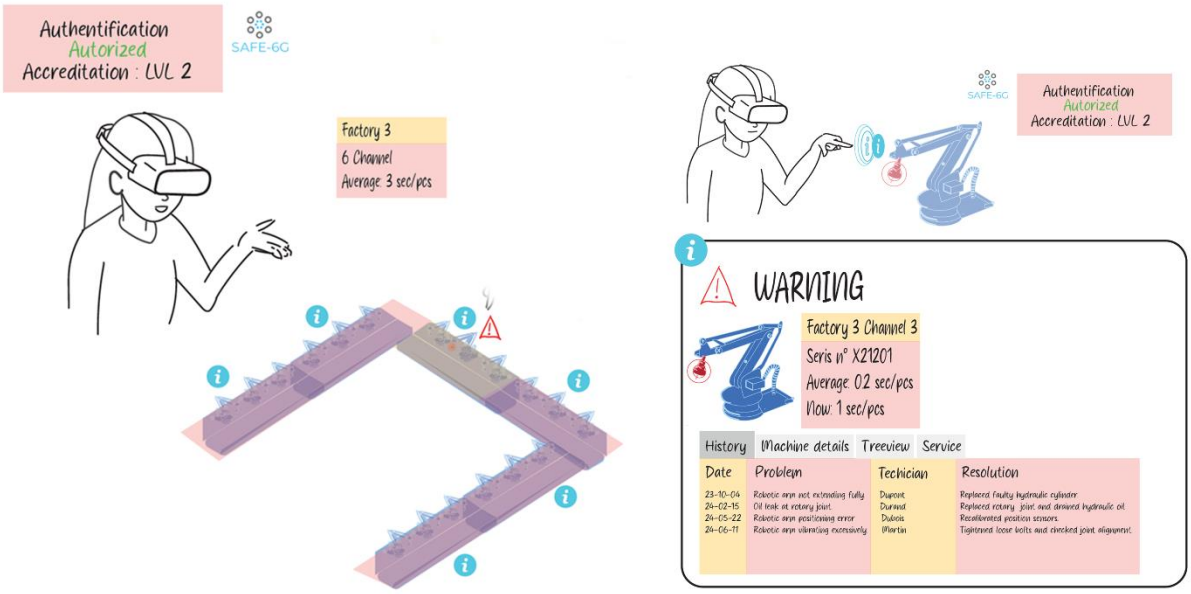

Figure 5: The director has all accesses to the DT. When she is connected to the metaverse application, she can see the whole factory in XR. She can also access the complete maintenance logs of machines.

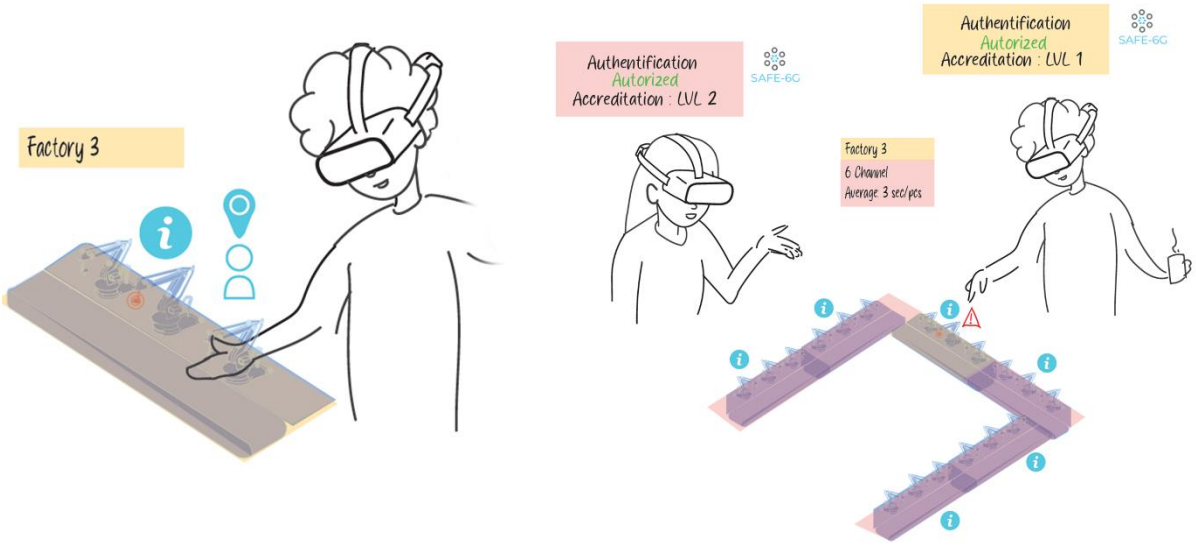

Figure 6: The manager only has access to the information of the line he is responsible for. Both users can nonetheless collaborate in real-time in XR.

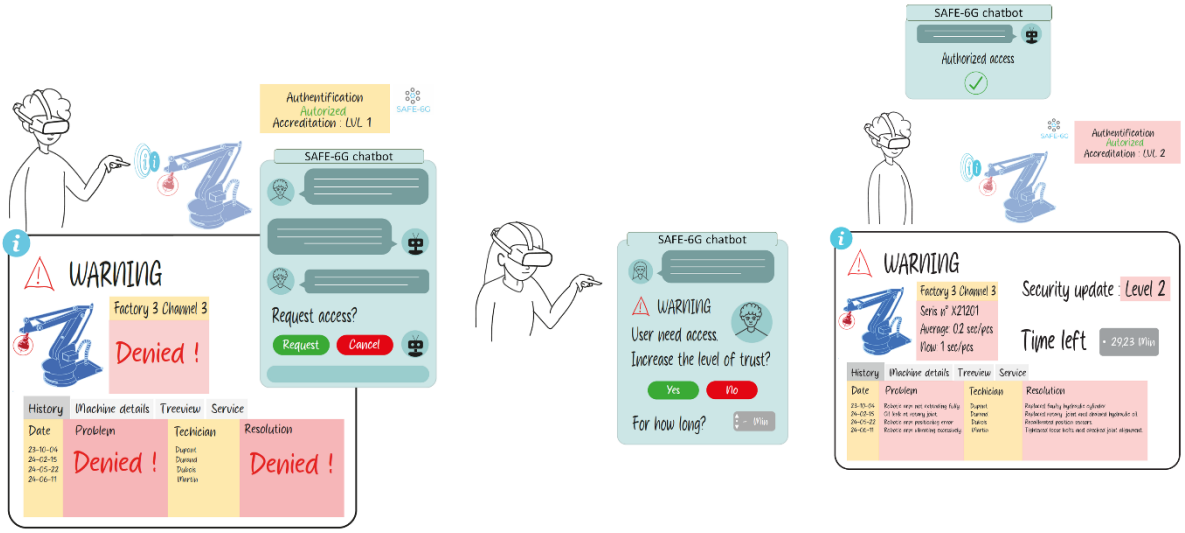

Figure 7: If needed, the manager can request access to more data by using the SAFE-6G chatbot. Upon acceptance on the director's side, the Level of Trustworthiness (LoTw) of the manager is temporarily elevated.

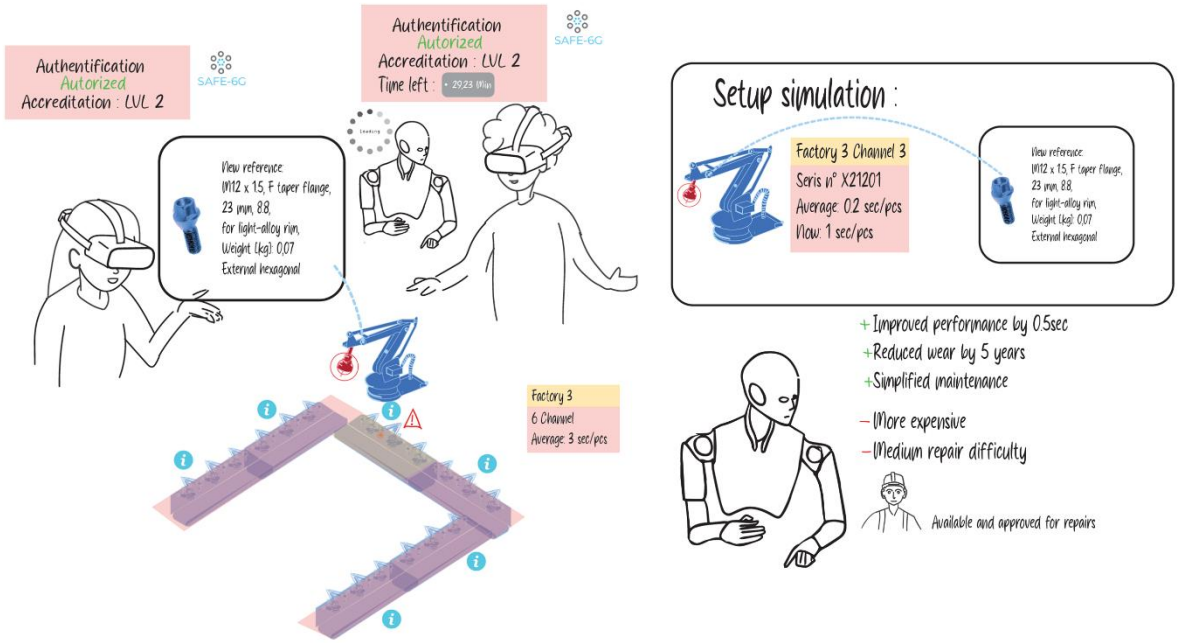

Figure 8: While they collaborate to design a solution, the users can interact with the IMM AI agent. This agent allows to run simulations and evaluate the impacts of proposed solutions.

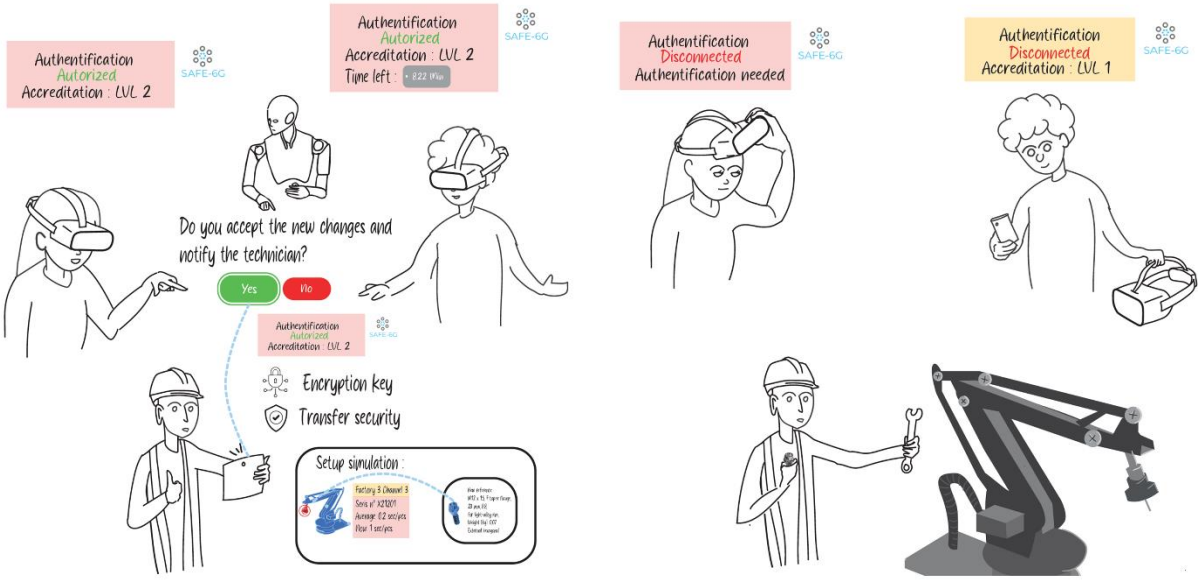

Figure 9: When a suitable solution is found, the director checks that the digital replica of the production line is correctly updated. The on-site technician can then proceed with the changes.

This overall scenario will be used as the main reference to design the concrete, step-by-step scenarios that will be conducted during the test phases of the project to demonstrate the SAFE-6G capabilities. These demo scenarios will be based on a simulated factory DT (but will be executed on a real Unity

application and real XR device). An example of such an envisioned scenario is presented below in Table 1. **The technical setup with envisioned XR devices, software components and technical architecture is detailed in Section 4.4.**

Step #	*Description*
1	The Production Director is notified of an issue in the factory DT. She puts her XR headset on, launches the UC1 metaverse application and authenticates herself to start a session.
2	The production director wants to visualize sensitive factory data. She thus uses the SAFE-6G chatbot to define her priorities, requesting for instance the highest level of security possible.
3	The SAFE-6G chatbot processes the text provided by the production director. Their intents are then identified through the intent classification component. If his intent isn't clear, the chatbot will prompt further questions until the intent is fully understood. Then, the Cognitive Coordinator quantifies the user intents to a score and calculates using the Reasoning Engine the Level of Trustworthiness (LoTw). After that, each trust function receives a coefficient of the LoTw, and each trust function performs an action based on the received coefficient.
4	The Production Director receives a notification in the chatbot. The notification gives a high-level confirmation that the network has given priority to Security aspects thanks to the explainable AI (XAI) aspects of the SAFE-6G framework.
5	The line manager tries to join the session, but the SAFE-6G network detects that his connection is not secured enough (ex: public Wi-Fi network). The production director is notified of the situation.
6	The production director finished checking a few sensitive data on the faulty machine, then closes all sensitive XR content. She then tells the chatbot that it is now acceptable to lower Security requirements as she just wants to discuss with the line manager.
7	When the SAFE-6G network has successfully handheld the request, the line manager is finally authorized to join the session.

Table 1: Example of envisioned demo scenario for UC1.

2.1.2 USE-CASE 1 STAKEHOLDERS

The asymmetry between the production line manager and the production director is also reflected in their respective personas. Personas are fictional representations of a character with social, technical and psychological attributes, made to reflect a specific type of stakeholder. In the following, all persona pictures were created from generative AI [1] .

For UC1, the Line Manager persona (Figure 10) highlights the fact that this type of user is more concerned about the technical aspects. Their objectives focus on quickly addressing the issue by finding an appropriate solution. Their expectations about the 6G network mainly consist in getting a suitable Quality of Service (QoS) to work efficiently in a secured environment. They thus emphasize Performance, Security and Reliability aspects. Line managers also have limited accreditations levels on the factory DT, with access restricted to only their production line machines and worker information.

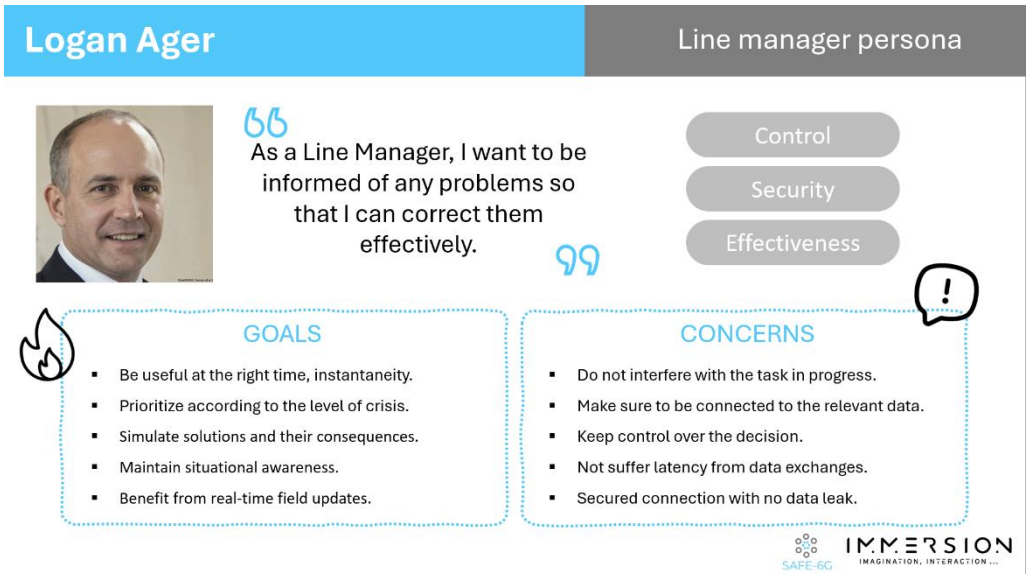

Figure 10: Line manager persona for UC1.

The production director persona reflects more general concerns about factory processes. While they also consider technical aspects of a given production line, they may prioritize aspects related to data privacy, traceability, and global optimization of the factory workers and machines. Overall, their expectations towards 6G networks may be more oriented towards Privacy and Resilience than line managers. Production directors also have full access to the factory DT, with the ability to check other production lines and history information about employees and machines. Such a high accreditation level calls for appropriate authentication and security mechanisms that are more advanced than those for line managers.

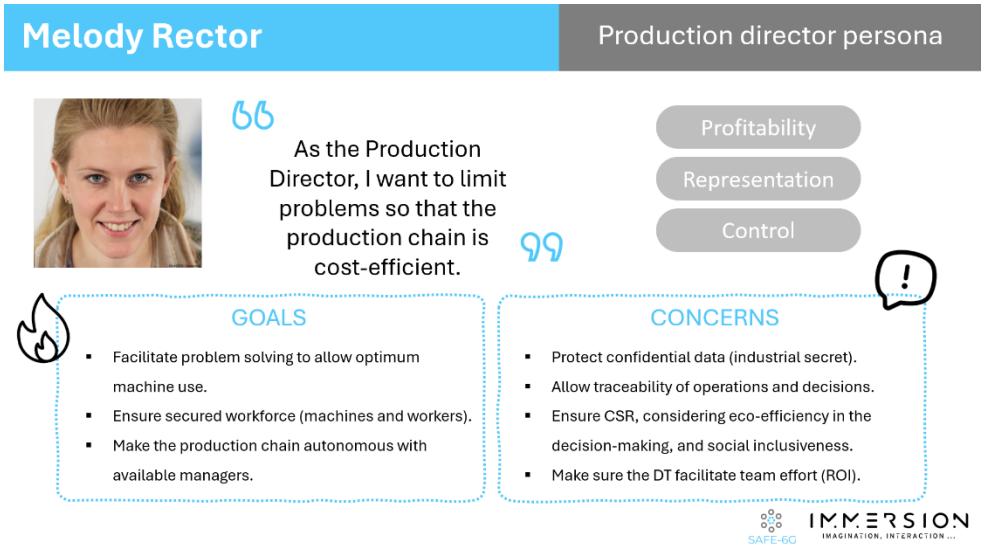

Figure 11: Production Director persona for UC1.

Despite these differences, the two user profiles have similar requirements in terms of XR devices. Performant wireless headsets are required to allow them to visualize factory data in XR and collaborate until a solution is defined.

2.1.3 Benefits of SAFE-6G for Use-Case 1

The first benefit of SAFE-6G for the first use-case is to bring state-of-the art network performances to XR collaboration. Factory DTs involve significant volumes of data to accurately reflect complete factory products, machines and complex industrial processes. Pre-recorded data (for instance, 3D scans of production lines made to record precisely the configuration of each production area) are often combined with real-time data from machine sensors. The evolution of each piece of equipment can also be finely monitored, which implies archiving time data as well. Overall, both the Production Director and the Line Manager need to access real-time and in a reliable manner to a huge amount of past and present data. The 6G network can offer a satisfying QoS to allow these end-users to collaborate in real-time in XR with a low and stable latency, a suitable framerate and an appropriate throughput.

However, the benefits of SAFE-6G go far beyond the level of performance offered by the network. By focusing on Trustworthiness, SAFE-6G aims at improving the trust users to accept to put into the system. Currently, many DT applications are hosted directly on factory premises. While it makes sense for Industry 4.0 companies to keep full internal control of their data and how it can be accessed, it also imposes limits on what is achievable remotely. Proposing a more trustworthy network that can be tailored to the needs of users can encourage them to remotely connect to their DT through XR applications. This could imply quicker reaction times when an issue arises in the production line, a better understanding of the situation through XR visualizations and thus overall improved management of production lines. Besides, managing LoTw with SAFE-6G also means addressing by design the access to data directly on the network level, adding another security layer around sensitive factory data.

Overall, the trust in the network gained from SAFE-6G will facilitate taking full advantage of factory DTs and the adoption of XR applications made to support the work of end-users based on these DTs.

2.2 Use-Case 2: Education and Formation

2.2.1 Use-case 2 scenario

As detailed in D2.1, Use-Case 2 (UC2) takes benefits from XR and AI to facilitate the recording and transmission of knowledge from an experienced individual to a group of learners. More precisely, an instructor will first record a given machine procedure in XR. This recording will be presented to factory workers as the key learning resource. Then, workers can simulate and repeat the procedure in XR until mastering it, under the supervision of the remote instructor and helped by a guidance AI agent. Most UC2 steps remained the same during the second iteration in its scenario. Instead, this second iteration allowed to detail further the aspects linked to trustworthiness, which are at the heart of SAFE-6G.

The first developed aspect concerned user privacy. XR devices include a lot of sensors to detect their environment and react to user actions. Such sensors include for instance several cameras to detect the room features (walls, obstacles) and user gestural interaction to interact with virtual menus or trigger commands. Eye-gaze and pupilar activity data are also often collected in real-time by many XR headsets as they are great indicators of the attention and concentration of users. The collected data often does not raise any issue for co-located users, who can, in any case, see each other physically.

However, remote users may not want to share this data with others. This can for instance be the case for a collaborator working from home, who may need to share with their colleagues what they can see in XR without showing their home features. Privacy is thus a significant challenge for XR and giving a feeling of control over it to users can greatly impact the adoption of the system.

The second aspect added to the UC2 scenario was the prevention of cyber-physical attacks. During the second part of the formation, factory workers must perform simulated steps of the procedure until mastering it. This implies working with both virtual and physical objects, tools and machine replicas. An attacker gaining control of physical devices could create harm to workers. For instance, one of the devices envisioned to support the learning phase and the level of immersion of the experience are the TouchDiver G1 [2] haptic gloves from WeArt. These haptic gloves can create different types of feedback, including thermal feedback on fingertips to simulate touching cold and hot virtual surfaces. Feeling the heat from machine parts can be valuable feedback for technicians, but an attacker could create physical discomfort for users. This second aspect is thus linked to both Security and Safety.

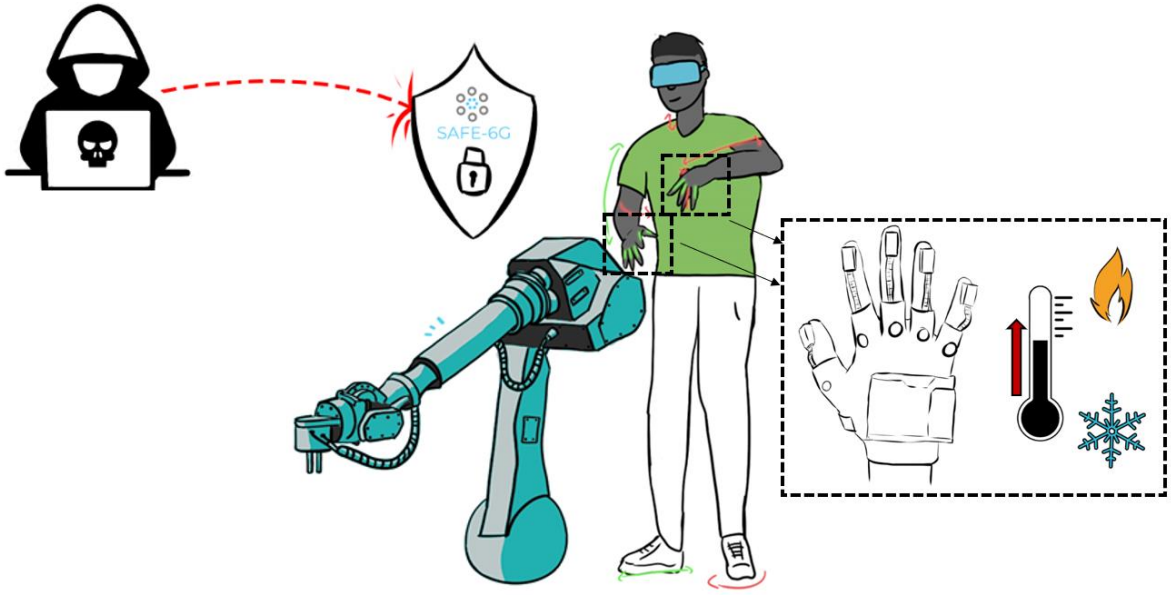

Figure 12: Example of potential cyber-physical attack for UC2. An attacker could try to take control of the thermal feedback provided by the user's haptic gloves to cause physical harm.

The first envisioned demo scenario is detailed in Table 2. Similarly to UC1, demo scenarios will be simulated (*i.e*. not performed with the actual end-users following a real formation session) but run on real XR devices during validation activities. They will be revised and completed according to the progress of SAFE-6G components implementation. **The setup for UC2 with envisioned devices, software components and technical architecture is detailed in Section 4.5.**

Step #	*Description*
1	A formation session started. Technicians are watching the recorded machine procedure through their XR headsets, and the instructor is there to answer potential questions.
2	Practical training starts. Technicians are now redoing the procedure step-by-step in XR, working in small groups of two with dedicated Netcode [3] sessions. Technicians working together tell the chatbot that privacy can be temporary lowered.
3	The SAFE-6G system handles these requests, performs the corresponding changes and provides a high-level notification to end-users through the chatbot.
4	The instructor requests through the chatbot to maximise privacy since she is working remotely.
5	The SAFE-6G system detects that this level of privacy could not fully be reached for that user and that a compromise had to be made. A high-level explanation is provided to the instructor thanks to the XAI component of the SAFE-6G architecture.

Table 2: Example of envisioned demo scenario for UC2.

2.2.2 USE-CASE 2 STAKEHOLDERS

The first persona of the UC2 scenario is the *Instructor*. Instructors are experienced workers or professional trainers who want to transmit their knowledge to other colleagues. Their motivation is built around the desire to transmit truthfully and efficiently their skills. They need to trust that the procedure recording will faithfully capture the complexity of machine procedures. Security and Safety are among the most important trustworthiness aspects for them. For instance, an attacker poisoning machine procedure recording could mislead learners and cause physical harm in the factory. Instructors have elevated access and administration rights. They are the ones who create and edit formation content, create collaborative sessions and monitor the activity of learners.

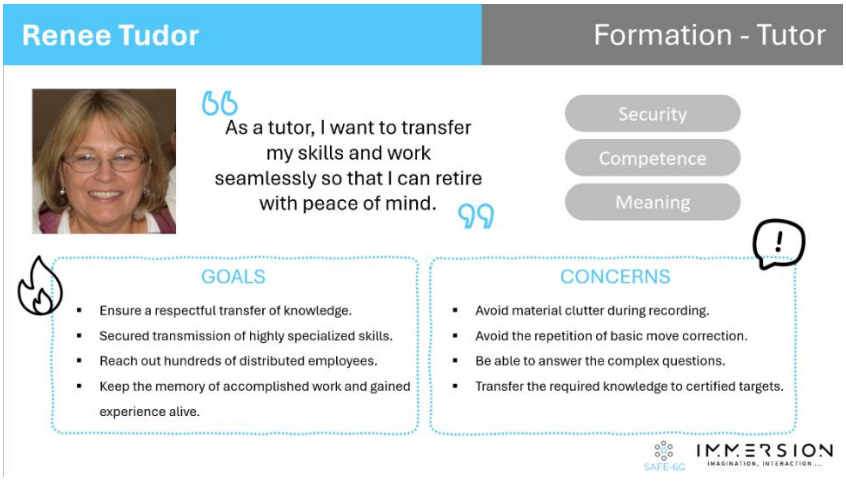

Figure 13: The instructor persona for the second use-case.

The second persona designed for UC2 is the *factory worker*. As learners, these users value gaining access to specialized knowledge and the actualization of their professional skills. They may be mainly interested in the high level of performance 6G networks have to offer. Nonetheless, Privacy aspects are also important to them as Industry 4.0 already involves more and more digital systems and data circulating within factories. Finally, paying attention to the technological inclusivity of the system is crucial for its adoption, as workers can have a broad range of experiences, expectations and apprehensions about new technologies. Factory workers, as learners, have more restricted accreditations than Instructors. They can access (but not edit) to formation and lessons content, join sessions and manage their own data.

Figure 14: The Factory worker persona for the second use-case.

2.2.3 Benefits of SAFE-6G for use-case 2

Similarly to the first use-case, the benefits of SAFE-6G for the second use-case include but are not limited to high-end performance levels. The notion of Trustworthiness involves several aspects for this use-case. Of course, the security and integrity of users and data are important for Education and Formation applications. Only verified users should be able to access the course content. It is for instance mandatory for formations leading to official certifications to ensure that only the proper users follow the training phases on machine procedures. Menacing the integrity of data could also lead to confusion, errors and even safety issues.

Privacy is another strong aspect linked to trust for UC2. XR technologies involve a lot of sensors collecting contextual and personal user data. Such data include 3D scans of the environment, real-time viewpoint from the XR headset, body postures, hand gestures, and eye-gaze activity. Some Virtual Reality (VR) headsets like the HP Reverb G2 Omnicept Edition [4] even collect biometric data such as heart rate. Allowing to request a given level of privacy to the network may comfort remote users that they have control over what they share with others. This is an important criterion for the adoption of the system, especially for users who may not yet have a strong experience in computer science, networks and/or immersive technologies.

2.3 How SAFE-6G functions enhance the use-cases

One of the goals of deliverable D2.1 was to provide an initial overview of the SAFE-6G concepts. D2.2 presented later the architectural components of SAFE-6G. This split was designed for clarity purposes to facilitate the traceability of concepts, components and common system requirements. The current deliverable goes a step further by precising the connections between these two approaches through the lens of the two metaverse use-cases.

As detailed in D2.2, SAFE-6G promotes a user-centric distributed 6G ecosystem. The network architecture should thus reflect the expectations and needs of end-users by providing personalized, secure, and reliable services. Within SAFE-6G, this is achieved thanks to the five Trust Functions (TF): Security, Safety, Privacy, Reliability and Resilience. Figure 15 provides examples of mapping between use-case needs and the SAFE-6G TF.

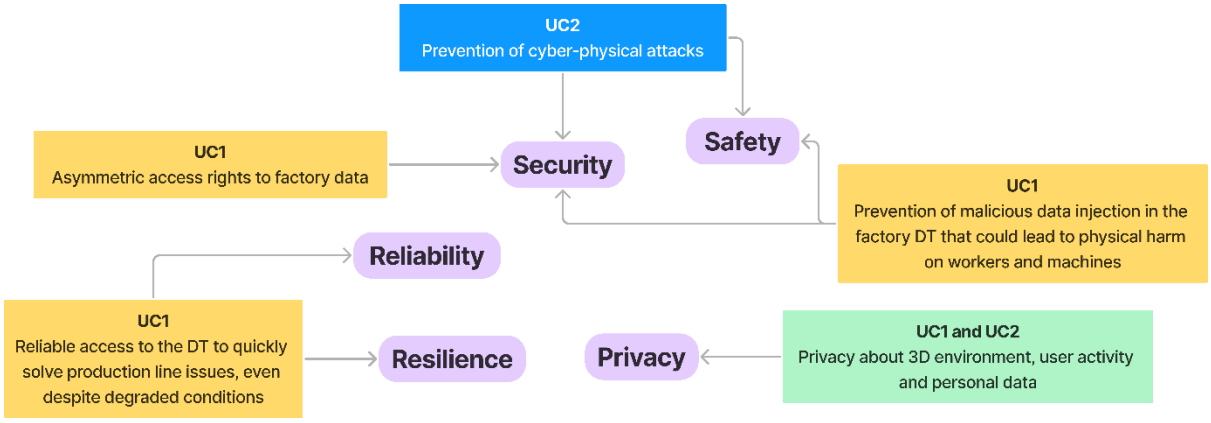

Figure 15: Examples of mapping between initially identified user needs and SAFE-6G Trust Functions.

Security is the most straightforward network function expected by end-users. Both use-cases involve remote access to resources (factory data for UC1, formation content for UC2) from authenticated users. More precisely, continuous authentication mechanisms are required for both use-cases to monitor the identity of each user during the whole usage of metaverse applications. Data breaches and identity theft are major threats that could discourage end-users from adopting a new system based on 6G networks. Without a secured-by-design solution to manage access rights and the actions of users, interacting with a factory DT like in UC1 is simply not possible, even with on-premises deployments. Besides, UC1 introduces an asymmetry between the metaverse application end-users namely the *Production Director* who has a global view of all production lines, and *Production Line Managers* who are dedicated to a single production line. As a result, the *Production Director* can access the entirety of the production line DT while the *Production Line Managers* only the services that are linked to his Line. At the same time, they both need to collaborate efficiently in XR despite not having the same features and authorizations in the factory DT. Any breach of this hierarchy can lead to corruption or leaks in production information such as time plans, resources and protocols used, budgeting information and so on. The cost of such a breach can result in significant delays in production, not to mention misuse or exploitation of the information by third parties.

The SAFE-6G Security TF and its zero-trust core concept is thus the first mandatory step to convince end-users that a 6G-based solution can address their need for transparent and secured management of sensitive data.

Safety, in the context of SAFE-6G use-cases, is directly linked to the potential physical harm done to humans and damage done to equipment. An intruder taking control of even a fraction of a factory DT in the context of UC1 could affect the behaviour of production line machines and harm workers. Production directors and line managers would simply refuse to use a system in which their collaborators could be harmed. Similarly, factory workers need to be able to trust that the persons in charge will ensure their physical safety. Any doubt about this basic requirement could severely impede the psychological well-being of workers and the collaboration between team members. Similarly, cyber-physical attacks on XR devices could create discomfort or even pain for technicians. Safeguard mechanisms to isolate network components and minimize the risks of safety threats are thus mandatory and will be handled by the SAFE-6G Safety TF. Moving beyond the primary target of reassuring the physical protection of the personnel within the factory, the contribution of the Safety Function to the wellbeing of the eco-system, spans to all the aspects of the factory's production process.

By controlling the microservices to which each stakeholder has access during the training, the Safety Function reassures that only the assigned users can access the training material while in the case of an infiltration, the malicious users cannot have access to the entity of the company's resources. The proposed AF is tailored to function seamlessly with SAFE-6G's 6G Packet Core and provide protection to all infrastructure nodes in this case production resources, machines robots etc., by giving access only to the microservices that are relevant to the assigned users.

Privacy also seems to be a straightforward requirement for both use-cases. UC1 involves sensitive factory data and industrial secrets while UC2 is based on private formation content about sensitive procedures. However, the need for privacy goes a step beyond with the usage of XR devices. Similarly to UC1, the training process in UC2 contains the transfer of sensitive information as it foresees the transfer of and expert's know-how to others. Such know-how is often a sensitive asset of a company as it takes years to be built and can often be the element that positions this company in the market. A potential infiltration of a malicious user in the training process can result to significant compromise to the company's know-how and lose of its competitive advantage in the market. In addition, during the training process, the company's resources are revealed to the trainees, resources that are often part of its intellectual property and are to be disclosed only to members of the company's crew. Trainers often have a wide range of those resources at their disposal as part of the different training modules they deliver while the trainees' access to it must be limited to the material that is relevant only for the specific training.

To ensure adequate privacy during the session, the privacy function operates at the network level, securing data transmission and access control mechanisms. This function prevents unauthorized data interception. By implementing robust confidentiality management, it mitigates risks associated with sensitive data exposure and maintains compliance with stringent privacy standards. The system dynamically enforces policies that restrict access based on predefined security parameters, ensuring

that user interactions within the XR environment remain protected while maintaining the integrity of company assets.

Reliability is more critical for UC1 than for UC2. For the latter, having an unreliable system may require rescheduling the formation to an ulterior date, as the certification on the machine procedure cannot happen in degraded conditions. However, for UC1, an unreliable system would, in the best scenario, defeat the purpose of the DT: it would not be possible to monitor properly the factory, run simulations, or remotely adjust a production line. In the worst scenario, an unreliable system could create confusion for the production directors and line managers, leading to erroneous decisions. Such decisions could create new issues and damages on top of the original issue on the faulty production line instead of solving it. The end users of UC1 thus need to trust that the factory DT will be accessible and deliver them the right, up-to-date factory data they need to quickly respond to production line issues. The SAFE-6G Reliability TF will thus be important for (mostly) UC1 to guarantee a robust detection of abnormalities and malicious behaviours at run-time to let end-users take the right course of actions.

Resilience, like Reliability, is mostly required for UC1. In the context of UC2, a system failure or strong degradation could simply require postponing the rest of the formation until the system recovery is complete. Potential consequences could be much more critical for UC1. Despite degraded conditions, production directors and production managers would still need to interact with the factory DT if the production line issue calls for a quick intervention. Being able to adapt to the needs of these users to transparently provide a suitable and continuous service delivery is thus expected from the network. In the context of UC1, the end-users are already under pressure from an issue detected on a production line for which they are responsible. They thus need to fully trust that the network system will not create additional difficulties for them. Within SAFE-6G, this will be achieved through the Resilience TF.

Section 3 goes one step further by describing in more details the requirements, KPIs and KVIs emerging from both use-cases.

3 USE-CASE REQUIREMENTS

Using the final scenarios and stakeholders described above, a set of end-user requirements, reference QoS metrics and KVIs have been designed to further define and categorize the expectations of end users for the SAFE-6G system. Some of these requirements are common to the two use-cases while others only concern one of them.

This section focuses only on requirements, metrics and KVIs from the perspective of end-users. The KPIs and KVIs related to the rest of the SAFE-6G architecture are detailed in D2.4.

Besides, the resolution of conflicting requirements, handheld by the Cognitive Coordinator (as mentioned in D2.1), will be presented in a future WP3 deliverable. The technical aspects of this resolution are beyond the scope of the end-user perspective, who only need to be informed in a high-level way about the compromises made (see REQ-USER-Both-F-NF-3 below).

Template field	Description
ID	A unique ID in the form REQ-COM-CATEGORY-TYPE-PRIORITY-#
Domain	DOMAIN = USER
Category	Category = UC1 | UC2 | Both UC
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

Table 3: Common system categories.

3.1 SHARED REQUIREMENTS

Template field	Description
ID	REQ-USER-Both-F-M-1
Domain	**DOMAIN = USER** USER: User and Use case
Category	Both UC
Requirement type	**Requirement type = F**
Priority	**Priority = M (Mandatory)**
Short title	The system should check the digital identity of users before granting them access to the session
Description	Authentication is a strong requirement for both use-cases. Continuous authentication is important since users should not be able to pass their XR device to another, non-accredited user.

Template field	Description
ID	REQ-USER-Both-NF-R-1
Domain	**DOMAIN = USER** USER: User and Use case
Category	Both UC
Requirement type	**Requirement type = NF (Non-Functional)**
Priority	**Priority = R (Recommended)**
Short title	Making sure end-users can still easily connect to the SAFE-6G network despite all security/trust measures
Description	It is important to facilitate as much as possible the connection to the SAFE-6G network for end-users to avoid disturbing their workflow. The use-cases already involve a significant level of new technologies and devices. If the procedure to connect to the 6G network and be authenticated is too tedious, end-user adoption may be significantly impacted. Examples: Typing long passwords on virtual XR keyboards is often cumbersome and error-prone (no haptic feedback, etc). Initially envisioned KPI: User authentication time <= 20s

Template field	Description
ID	REQ-USER-CATEGORY-Both-NF-M-2
Domain	**DOMAIN = USER** USER: User and Use case
Category	**Both UC**
Requirement type	**Requirement type = NF**
Priority	**Priority = M (Mandatory)**
Short title	Security and trustworthiness measures should not disturb significantly the work of end-users
Description	Both use-cases target contexts where security, safety and trustworthiness are key. End-users thus know that they must respect some procedures and constraints. Nonetheless, their work should not be too much disturbed by these concerns. Corresponding KPIs could include overall task completion times, mental workload and usability scores.

Template field	Description
ID	REQ-USER-CATEGORY-Both-F-R-1
Domain	**DOMAIN = USER** USER: User and Use case

Category	**Both UC**
Requirement type	**Requirement type = F (Functional)**
Priority	**Priority = R (Recommended)**
Short title	The SAFE-6G chatbot should check for input attacks
Description	Letting end-users interact on the fly with the SAFE-6G chatbot to adjust LoTw levels requires making sure this interaction is secured. In particular, the chatbot should be protected against input attacks (in which the data/requests fed to the AI system are manipulated to affect the output in a way desired by the attacker). For instance: malicious input/injection through the chatbot to modify the trust level of another user without his/her consent.

Template field	Description
ID	REQ-USER-CATEGORY-Both-NF-O-4
Domain	**DOMAIN = USER** USER: User and Use case
Category	**Both UC**
Requirement type	**Requirement type = NF**
Priority	**Priority = O (Optional)**
Short title	End-users should be able to understand the decision of AI agents
Description	AI explainability is a significant challenge for the adoption of such technology. In the use-cases, the end-users may have limited previous knowledge and experience with AI agents. Nonetheless, they need to be able to understand which factors motivated the decisions from the SAFE-6G system. This is applicable to both the SAFE-6G chatbot handling LoTw and the IMM AI agents, but explainability for the SAFE-6G chatbot has the priority. Examples: asking in the chatbot why an AI decision has been made, having a Graphical User Interface to illustrate its “thought process” and see which dataset was used for training, etc.

Template field	Description
ID	REQ-USER-Both-F-NF-3
Domain	**DOMAIN = USER** USER: User and Use case
Category	Both UC
Requirement type	**Requirement type = NF**

Priority	**Priority = M (Mandatory)**
Short title	In case of conflicting and/or unattainable requirements, the system should warn the user in a high-level way
Description	End-users may perform requests that enter in conflict with their attributed role, or which currently cannot be satisfied by the system. In such cases, the priority for users is to be notified in a high-level, non-technical way that a compromise had to be found or is proposed by the system. One way to do so could be to use the chatbot to explicitly ask the user what his/her priority is between the conflicting aspects

3.2 REQUIREMENTS FOR USE-CASE 1

Template field	Description
ID	REQ-USER-UC1-F-R-1
Domain	**DOMAIN = USER** USER: User and Use case
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = F**
Priority	**Priority = Recommended**
Short title	Check that DT data come from appropriate locations
Description	The manager needs to be sure that the data alimenting the DT comes from worker/sensors from the factory. One way to check that is to track the location of UEs/IoT and make sure they correspond to the correct factory, production line or machine. Different levels of precision can be envisioned: factory level (+- 30m), production line level (a few meters) or machine level (1m precision).

Template field	Description
ID	REQ-USER-UC1-F-R-2
Domain	**DOMAIN = USER** USER: User and Use case
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = F**
Priority	**Priority = R**
Short title	Check that the manager has access only to the required data
Description	Even when authenticated, production line managers should not have access to factory data that is not required to address the issue. The less sensible data is transmitted through the network, the better.

	The transmitted DT data should thus 1) depend on the LoTw related to the manager and 2) be as much on-demand as possible. Zero Trust architecture principles should be followed. Punctual and contextual anomaly detection could be a way to monitor that the user accesses or requests access to relevant data only (and not downloading a large range of DT data from another production line for instance). Data breach detection would also be interesting.

Template field	Description
ID	REQ-USER-UC1-F-R-3
Domain	**DOMAIN = USER**
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = F**
Priority	**Priority = R**
Short title	The system must check that sensitive data are correctly encrypted
Description	This requirement is linked to the previous one. Since factory data can be highly confidential and sensitive (including secret industrial processes), the system needs to actively check that all communication between trusted devices is correctly encrypted. If possible, the system should also check that this encryption is not leveraged by an attacker (using encrypted malicious payloads).

Template field	Description
ID	REQ-USER-UC1-F-M-4
Domain	**DOMAIN = USER**
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = F**
Priority	**Priority = M**
Short title	The system must monitor the manager activity to detect malicious behaviours
Description	This requirement is linked to REQ-USER-UC1-F-R-2 but focuses on the user's activity more than data. The manager is supposed to only work on the detected production line issue. Making other non-related changes, like editing DT logs or configuration files should be flagged as suspicious activity and treated accordingly, for instance by a host intrusion detection system or equivalent.

	This may be difficult as the issue detected on the production line is an anomaly event and solving it may require specific adaptations.

Template field	Description
ID	REQ-USER-UC1-NF-M-5
Domain	**DOMAIN = USER**
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = NF**
Priority	**Priority = M**
Short title	Check that the solution proposed by users is suitable
Description	Users will propose changes in the DT to address the initially detected issue. The system must check that these changes are appropriate, i.e.: • Will solve the issue • Will not create any other issue, harm on workers/machines or introduce malicious behaviours • If possible/applicable: respects a set of criteria like production efficiency, energy consumption, etc

Template field	Description
ID	REQ-USER-UC1-NF-R-6
Domain	**DOMAIN = USER**
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = NF**
Priority	**Priority = R**
Short title	DT services must be available when the manager is notified
Description	Service availability and reliability are crucial during a manager's intervention to ensure quick and reliable access to the relevant data. An acceptable level of QoS should be met to ensure real-time work in XR. Besides, attacks like Deny of Service on the DT would block the manager from intervening and could cascade issues inside the factory. Initially envisioned KPI: see Reliability and Availability performance metrics in Section 3.4.

Template field	Description
ID	REQ-USER-UC1-F-R-7
Domain	**DOMAIN = USER**

Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = F**
Priority	**Priority = R**
Short title	The system must check the coherency between the real factory and its digital replica
Description	If the digital part of the digital twin does not reflect properly the current state of the real factory, then the manager may make wrong assumptions and take poor decisions during the intervention. The system should thus check the consistency of data between the two. This could be achieved on several aspects: • Checking that the digital part is synchronized and up to date • Checking anomalies and inconsistencies (for instance, a machine being flagged as out of order and turned off, but products are still being processed as if it was functioning normally).

Template field	Description
ID	REQ-USER-UC1-F-R-8
Domain	**DOMAIN = USER**
Category	**UC1** (Digital Twin)
Requirement type	**Requirement type = F**
Priority	**Priority = R**
Short title	The Production Director should be able to temporarily elevate the accreditations rights of the Line manager
Description	As illustrated in Figure 7, the Production Director may want to elevate the accreditation rights of the Line manager. Such feature is related to the UC app in itself but may impact the LoTW attributed to the Line Manager. The SAFE-6G system should thus be notified of the change to be able to adapt the potential role-based rules within TFs.

3.3 REQUIREMENTS FOR USE-CASE 2

Template field	Description
ID	REQ-USER-UC2-F-R-1
Domain	**DOMAIN = USER** USER: User and Use case
Category	**UC2** (Education)
Requirement type	**Requirement type = F**
Priority	**Priority = Recommended**
Short title	Letting the instructor adjust punctually security/trust levels of the application

Description	An administrator should already have used the SAFE-6G AI agent (chatbot) to define desired levels of trust, security, etc. But the instructor may need to adjust them on the fly, for instance to give a special lesson to a sub-group of technicians who have a specific certification or to punctually demonstrate something more confidential.

Template field	Description
ID	REQ-USER-UC2-F-R-2
Domain	**DOMAIN = USER** USER: User and Use case
Category	**UC2** (Education)
Requirement type	**Requirement type = F**
Priority	**Priority = Recommended**
Short title	Letting end-users control the level of privacy of their data
Description	XR users can share much information about their surroundings: video streams, audio, 3D mapping of the room, etc. It is important to let users in control of what they share with others. But in additional to this “manual” control, it would be great if the system could also ensure that these data streams are visible only for the appropriate users. Example: a remote technician sharing its video stream with some colleagues only. Or blocking the sharing of biometric signals (heart rate, pupilar activity, etc) normally used to estimate stress levels and cognitive load.

Template field	Description
ID	REQ-USER-UC2-F-M-3
Domain	**DOMAIN = USER** USER: User and Use case
Category	**UC2** (Education)
Requirement type	**Requirement type = F**
Priority	**Priority = Mandatory**
Short title	Protecting the procedure recordings against data & model poisoning
Description	The demonstration recorded in advance by the instructor will feed the metaverse app and be used as a reference for the formation and the IMM agent AI training. It is thus crucial to ensure that this data was not biased/poisoned by a malicious user. Example of measures: re-checking the identity of instructor, location and coherency of recorded data compared to expected values...

Template field	Description
ID	REQ-USER-UC2-F-M-4
Domain	**DOMAIN = USER** USER: User and Use case
Category	**UC2** (Education)
Requirement type	**Requirement type = F**
Priority	**Priority = Mandatory**
Short title	Continuous authentication of the technician to be certified
Description	The system needs to make sure that only the appropriate person has access to the procedure formation. Non-authorized users should, of course, not be able to visualize any data about the factory and its processes. Moreover, the certification is strictly personal: it should not be possible to pass the certification for someone else (ex: giving the XR headset to another person). This is particularly important in critical systems, in which certifications are key to limiting hazardous human errors. Multi-factor identification may be envisioned (password + confirmation on another device, retina scan with XR headset...)

3.4 USE-CASE REFERENCE QOS METRICS

End-users have expectations about what the network can provide to allow them to perform their task in a fluid and efficient manner. In other words, the QoS provided by the 5G/6G network should not hinder the Quality of Experience (QoE) of the metaverse use-case applications. This subsection lists reference metrics for UC1 and UC2 in terms of minimum QoS. The goal of the SAFE-6G project is not to validate that the 6G network can go beyond these performance metrics for the two presented use-cases. **Instead, these metrics will be used during WP5 activities to validate that the SAFE-6G framework can maintain this minimum QoS expected by end-users on top of all its Trustworthiness features.**

Template field	Description	
Metric Category	Latency	
Short title	End-to-end latency between UEs	
Description	In both use-cases, end-users will work together in real-time in XR with virtual objects. The overall latency of the system should thus allow fluid collaboration between users connected to the 6G network.	
Use-cases	UC1	UC2
	<= 15ms	<= 20ms

Template field	Description	
Metric Category	Latency	
Short title	Latency jittering	
Description	Latency jittering is one of the most critical performance indicators for XR systems. Even limited latency spikes can affect real-time interactions with virtual objects. Not being able to predict the system latency prevents users from adapting to it, which creates confusion and greatly affects users' trust in the system. Overall, having a stable but higher latency is often privileged.	
Use-cases	UC1	UC2
	< 5ms	< 10ms

Template field	Description	
Metric Category	Framerate	
Short title	Number of frames displayed per second (fps) by XR devices	
Description	The number of frames rendered on the screen per second affects the fluidity of the XR experience and its comfort. This is especially important in VR to limit cybersickness. XR devices tethered to powerful workstations often offer a high number of fps (for instance, 90fps on Varjo XR-3 headsets). Nonetheless, both use-case scenarios encourage using wireless devices instead to preserve the mobility of end-users. The 6G network should thus offer suitable levels of performance to allow the cloud-rendered XR apps to reach a satisfying framerate.	
Use-cases	UC1	UC2
	>= 30fps	>= 30 fps

Template field	Description	
Metric Category	Bandwidth	
Short title	Downlink and uplink data volume (in Mbps)	
Description	Need to conduct performance tests with NVIDIA CloudXR to evaluate achievable results. An Ethernet-tethered workstation could process the data and stream the resulting frames to the XR devices.	
Use-cases	UC1	UC2
	>= 100Mbps downlink and 50 Mbps uplink	

Template field	Description	
Metric Category	Reliability	
Short title	Percentage of packet loss	
Description	The percentage of packets sent through the 6G network that do not reach their destination.	
Use-cases	UC1	UC2
	Comparable to URLLC systems	

Template field	Description	
Metric Category	Localisation	
Short title	Accuracy of the detection of UE localisation.	
Description	Required for REQ-USER-UC1-F-R-1. As mentioned in the description, several accuracy levels can be envisioned, with +- 1 meter as the most expected accurate level (machine level) if possible.	
Use-cases	UC1	UC2
	<= 5 meters.	Not required

Template field	Description	
Metric Category	Availability	
Short title	Percentage of time the system is operational.	
Description	Availability is much more critical for UC1 than for UC2. In UC1, the end users need to be informed as soon as possible when an issue is detected in the factory DT. An issue occurring during a system downtimes would be a low occurrence, critical risk for UC1. On the contrary, teaching or formation sessions could be more easily delayed if needed.	
Use-cases	UC1	UC2
	>= 99.99%	>= 99.9 %

3.5 USE-CASE KVIS

The definition of use-case KVIs followed the process proposed by the 6G-IA white paper [5] about the societal values 6G can address. After identifying stakeholders and societal pain points, positively impacted key values were extracted from use-cases. The potential scale of effect was then defined. Enablers and blockers were listed to precise the required leverages to use and barriers to overcome in order to reach the desired scale of outcome. **Finally, the KVIs are quantified with potential KPIs. These KPIs reflect desirable outcomes linked to the use-cases. Nonetheless, their validation is out of the scope of SAFE-6G as both use-cases will be based on simulated data instead of real environments and end-users. To be more precise, real XR devices connected to the SAFE-6G network will be used. The digital twin factory data (UC1) and the machine procedure formation data (UC2)**

will be simulated through their respective UC applications made in Unity. Real 6G testbeds will also be used at project partner premises (NCSRD, UPV and/or UNIWA). All details and results from the validation activities will be reported in P2 within the scope of WP5.

Template field	Description
Use case	UC1
Stakeholders	Industry 4.0 companies
Societal pain points	Do not trust external networks with sensitive factory data
Positively impacted Key Values	Trust, Privacy & confidentiality
Scale of effect: KVIs	Better acceptance rate (more users, deciding more quickly to get involved). Increase in the level of data sensitivity shared through the network.
Enablers and blockers	Secured-by-design network systems, built around trustworthiness. Visible indicators of the level of protection of the system.
Quantification with KPIs	Increase of +25% of users accepting to use the factory DT. Increase of shared data sensitivity (details about machines and workers, historical data about past failures)

Template field	Description
Use case	UC1
Stakeholders	Industry 4.0 companies
Societal pain points	Production line issues are not anticipated/corrected quickly enough
Positively impacted Key Values	Economical sustainability and innovation
Scale of effect: KVIs	Seamless and quicker decisions. Better explicability of decisions to improve processes over time.
Enablers and blockers	Accessible monitoring tools like DTs that can be used remotely
Quantification with KPIs	Factory production line updates decided in less than 20 minutes. Subjective feeling of better explainability of decisions (results from questionnaire)

Template field	Description
Use case	UC1

Stakeholders	Industry 4.0 companies
Societal pain points	Production line issues can result in human harm and significant economic costs
Positively impacted Key Values	Protection from harm, Economical sustainability
Scale of effect: KVIs	Less / No more work accidents and stops. Less productivity pressure on employees
Enablers and blockers	Factory DTs, visualization of health and productivity impacts
Quantification with KPIs	Work incidents of production line diminished by 25%. Overall production line uptime increased by 33%. Subjective work well-being of factory workers increased (evaluation through questionnaire)

Template field	**Description**
Use case	UC1
Stakeholders	Production directors and line managers
Societal pain points	Users are not always on-site when an issue arises
Positively impacted Key Values	Simplified life, Environmental sustainability (need to travel)
Scale of effect: KVIs	Improved acceptance of work (or personal) mobility
Enablers and blockers	Remote, secured access to factory data
Quantification with KPIs	+25% access to factory data from remote locations, -50% travels done by production directors and line managers to solve issues on production lines (evaluated after 2 years)

Template field	**Description**
Use case	UC1
Stakeholders	Production directors and line managers
Societal pain points	Do not trust remote operations to remotely perform changes on the factory through its DT.
Positively impacted Key Values	Trust, Protection from harm

Scale of effect: KVIs	Improved feeling of certitude about the benefits of proposed modifications. Increased number and amplitude of DT updates.
Enablers and blockers	Validation and simulation tools to check proposed DT updates, automated tests, advice from AI agent.
Quantification with KPIs	+25% DT updates performed after 1 year of use, including cases requiring significant production line adaptations.

Template field	**Description**
Use case	UC2
Stakeholders	Technicians
Societal pain points	Access to formation tools or courses at any time and within trusted environments is usually hard (except paper manuals for instance)
Positively impacted Key Values	Knowledge, Simplified life
Scale of effect: KVIs	Quicker access to technical information. Reduced usage of paper documentation (frequency and time spent)
Enablers and blockers	Metaverse solution: persistent formation content accessible from anywhere at any time, in a suitable form
Quantification with KPIs	–50% usage of paper documentation about the machine procedure after 1 year.

Template field	**Description**
Use case	UC2
Stakeholders	Instructors
Societal pain points	Hard to have efficient ways to keep record and maintenance of all their knowledge and expertise
Positively impacted Key Values	Knowledge, Simplified life
Scale of effect: KVIs	Increased completeness of recorded knowledge (including formal and informal information). Reduced time to archive knowledge and author formations.

Enablers and blockers	Access to multimodal archiving and formation authoring tools
Quantification with KPIs	Time required to record and archive a machine procedure reduced by 33%. Number of archived machine procedures increased by 25% after two years.

Template field	**Description**
Use case	UC2
Stakeholders	Instructors
Societal pain points	Hard to transmit their knowledge and expertise remotely in an efficient manner
Positively impacted Key Values	Knowledge, Environmental sustainability
Scale of effect: KVIs	Better knowledge transfer: reduced formation times and number of sessions. Increased number of remote formations
Enablers and blockers	Remote formation tools with optimized energy consumption
Quantification with KPIs	Machine procedure formation time and number of on-site formation sessions reduced by 25%. Number of remote formation sessions increased by 25%.

Template field	**Description**
Use case	UC2
Stakeholders	Instructors
Societal pain points	Hard to make sure that only the proper technicians will follow the formation and be certified in the end
Positively impacted Key Values	Trust
Scale of effect: KVIs	Automated system procedures: decreased time to check the digital identity of technicians
Enablers and blockers	Additional security built within the network itself to ensure the continuous authentication of learners

Quantification with KPIs	Overall time to authenticate remote technicians is less than 2s.

Template field	**Description**
Use case	UC2
Stakeholders	Instructors and technicians
Societal pain points	Want to have control over the personal data they share with others, ensuring the privacy of data and confidentiality
Positively impacted Key Values	Privacy & confidentiality
Scale of effect: KVIs	Granularity and number of adjustable privacy settings
Enablers and blockers	Network system allowing control Privacy levels, immersive apps with adjustable privacy settings.
Quantification with KPIs	At least three levels of privacy settings are available in the system. Better subjective feeling of privacy control for instructors and technicians (evaluated through self-report questionnaire).

Template field	**Description**
Use case	UC2
Stakeholders	Instructors
Societal pain points	Fear of knowledge leakage, theft of know-how
Positively impacted Key Values	Trust, Privacy, and confidentiality
Scale of effect: KVIs	The knowledge stays in the company / in the hands of chosen people: increased number of instructors accepting to create formations.
Enablers and blockers	Secured-by-design network systems, built around trustworthiness. Visible indicators of the level of protection of the system.
Quantification with KPIs	Number of instructors accepting to create formations increased by 25% after one year.

4 TECHNICAL DESIGN OF USE-CASES

4.1 TECHNICAL CONSIDERATIONS ABOUT XR DEVICES

Designing a technical system architecture first requires considering the capabilities and current limitations of current XR devices. The first type of limitation is the limited computational power of mobile XR devices (from smartphones and tablets to complete headsets). While high-end devices embed ever-improving hardware, they still pale compared to tethered devices linked to powerful workstations.

The second type of limitation is the connectivity of XR devices. Smartphones and tablets can easily be made compatible with 5G and 6G networks, but this is not the case for headsets. In fact, no commercially available XR headset can directly connect wirelessly to a 5G network. This is a strong limitation as it requires a 5G-enabled device to share its connectivity through a Wi-Fi hotspot, which significantly degrades the overall performance levels. Recent XR devices like the Vive XR Elite [6] and the Meta Quest 3 [7] now support the 6GHz band introduced in Wi-Fi 6E, but this once again is a technical step back compared to tethered devices.

One of the solutions to partially address this issue is to use a cloud-rendering service. This way, time-consuming computations are offloaded to powerful workstations where XR application is deployed. The resulting video frames are then sent to the end-user devices to be displayed. On the contrary, XR devices send back user interaction and data collected from sensors so that the application reacts to user input. The CloudXR solution from NVIDIA [8] has been identified and explored as a promising solution to achieve this paradigm. An on-premises configuration can be achieved if needed to facilitate tests with a 6G network deployed locally.

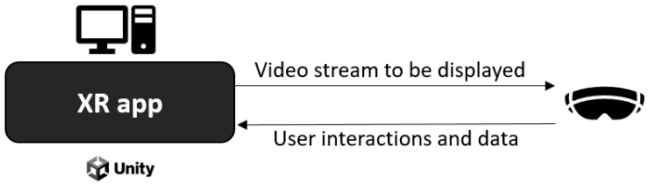

Figure 16: Overview of the functioning of a cloud-rendered XR application.

4.2 INTEGRATION WITH THE SAFE-6G CHATBOT

This section outlines the integration of the SAFE-6G chatbot with the metaverse applications, ensuring secure and dynamic interaction between users in the XR environment and the chatbot. The chatbot processes natural language free text inputs, recognizes user intent, and retrieves the appropriate LoTw that is calculated in the Cognitive Coordinator of the SAFE-6F framework.

APIs, such as the following, are going to be exposed by the chatbot backend to facilitate communication with the XR environment:

- **Intent Recognition API:** This API processes the user's free-text input to determine the intent. The metaverse application sends the input securely to the chatbot backend through API calls, which trigger the corresponding action based on the recognized intent.
- **Clarification Prompt API:** If the intent is unclear, this API prompts the user for additional information, ensuring that the system performs the intended action accurately.
- **Trust Level Explanation API**: After retrieving the LoTw, this API provides a detailed explanation of how the level of trustworthiness was determined, offering transparency to users within the XR environment.

The communication between the XR environment and the chatbot backend will be secured using the following, open-source security measures:

- **Transport Layer Security (TLS):** TLS encryption is used to secure all data exchanged between the XR devices and the chatbot backend. The system uses free SSL/TLS certificates from *Let's Encrypt*, ensuring that all communications are encrypted and protected against unauthorized access.
- **JSON Web Tokens (JWT):** JWTs are employed to authenticate users and secure API access. Free libraries such as *PyJWT* (Python) are used to generate and verify tokens, ensuring that only authenticated users can access sensitive functionalities like adjusting trust levels.
- **Input Validation**: The chatbot backend employs input validation mechanisms to ensure that data received from the XR environment is sanitized and safe. Libraries like Flask-WTF (Python) are used to validate and sanitize user inputs, protecting the system from injection attacks and malicious data.

These security measures ensure that communication between the XR environment and the chatbot remains secure, allowing users to interact confidently and freely within the SAFE-6G metaverse applications.

4.3 The Metaverse Manager Component

To facilitate the interaction with metaverse applications during the different validation phases of the project, an intermediate component could prove useful. The *metaverse manager* component was thus envisioned to provide endpoints and expose APIs to SAFE-6G components (including the chatbot). It consists of an intermediate Python application, as shown in Figure 17. The metaverse manager could be more easily containerized and deployed in project partner premises than metaverse applications to perform tests.

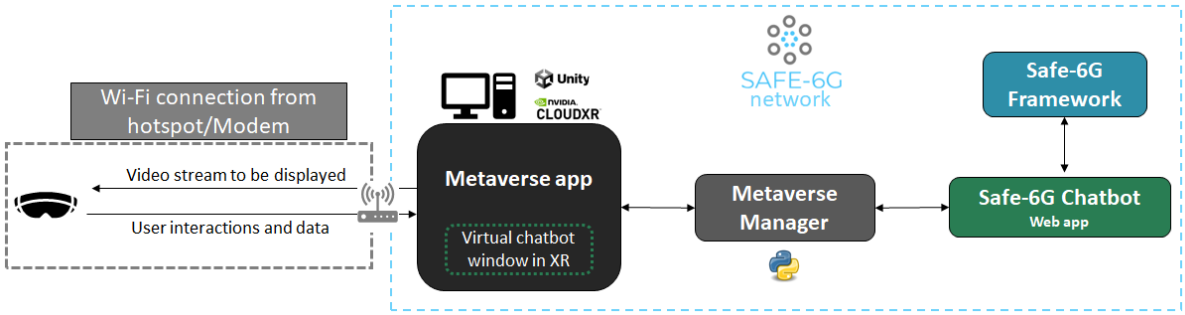

Figure 17: Overview of the main architecture components and their relationships.

As described in D2.2, the SAFE-6G chatbot will be displayed as a virtual window in XR. End users will be able to interact with it using a physical keyboard thanks to video see-through XR headsets. The metaverse application will then communicate the request of the user to the metaverse coordinator through TCP sockets. Exposed endpoints will then allow the metaverse coordinator to transmit the request to the SAFE-6G chatbot application, then receive the answer from the system and display it in the virtual window. This will be achieved thanks to web requests and custom APIs defined by the chatbot application and the metaverse manager.

The metaverse manager component will also be used to transmit data required by the TFs to the SAFE-6G framework. These data will include (but not be limited to) information about connected UEs and user roles. While the initial authentication procedure of the metaverse applications is based on dedicated user logins and passwords managed on the metaverse manager side, authentication and security mechanisms will be adapted along the course of the project to reflect the end-user requirements and the capabilities of the TFs.

4.4 Technical design for use-case 1

The main specificity of UC1 is that it involves a factory DT. Designing and integrating an application reflecting the state of a real factory is a complex, time-consuming process with many challenges. In addition to the 3D scans of the working environments, the DT must be coupled to different factory software to be able to collect sensor data, monitor in real time workflows and dataflows and perform simulations. Beyond the issues related to the sensitive nature of using real factory data, such a process is out of the scope of SAFE-6G.

Instead, simulated data will be used to reflect the behaviour of a factory with several production lines. A first Unity application (running on a real XR device) will thus be designed to play the role of the DT of this virtual factory.

The first envisioned architecture for UC1 was based on Nvidia solutions (in addition to CloudXR). Nvidia offers several rendering and collaboration tools, including for XR applications. Such tools are based on Universal Scene Description (USD) [9] . USD provides a common language for defining, assembling and editing 3D data, facilitating the use of multiple digital content creation applications. This approach is interesting for XR because it provides a standardized way to describe 3D scenes and makes them compatible with different applications. In the initially envisioned architecture, the 3D scene of the Digital Twin Unity application was supposed to be exported in USD to a Nucleus server. This way, end-

users (the Production Director and the Line Manager) could have a live access to the DT scene through the USD Composer tool and Unity connectors, allowing them to visualize the state of the faulty production line and collaborate to design a solution.

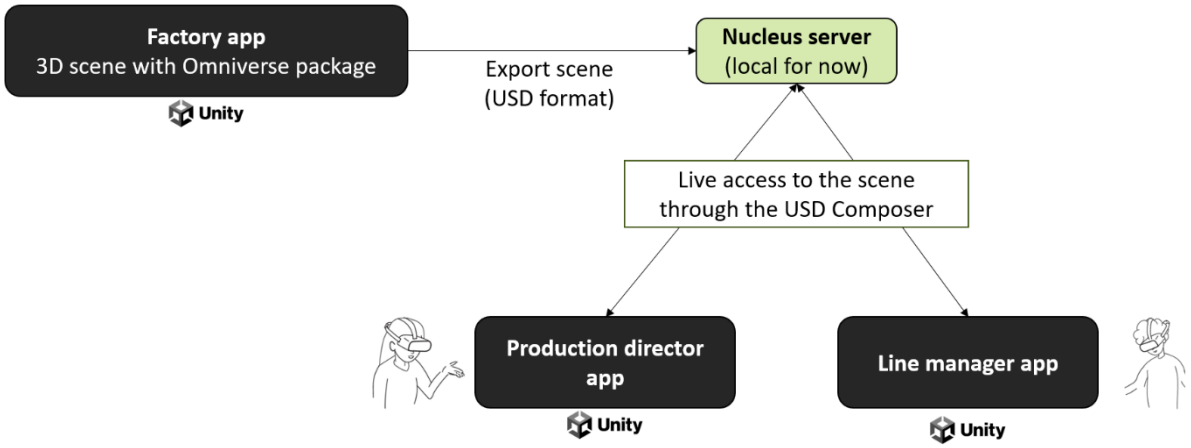

Figure 18: Initially envisioned architecture for the metaverse application of UC1.

However, early tests of this approach revealed two major limitations. First, the current version of Unity connectors provided by NVIDIA is not bidirectional. Changes performed on the DT side can be reflected in real time on the end-user side, but not the other way around. This is a strong limitation as it means end-users can only perform local changes. They cannot collaborate with each other nor push their designed solution to the factory DT. The second limitation is that the Nvidia USD Composer is not designed to run on workstations. XR devices do not have the computational power required to run it in a satisfactory manner. These two major limitations discouraged us from selecting this architecture for UC1.

Another approach based on Omniverse Create XR [10] by NVIDIA was also investigated within the project's framework. *Omniverse Create XR* offers powerful rendering capabilities to let XR users navigate in immersive 3D scenes with high-quality visuals (including raytracing, advanced shadow/lighting rendering and heavy 3D models). The tool uses CloudXR to stream the rendered scene to the targeted XR devices. The list of officially supported XR devices is nonetheless limited to two devices (the Meta Quest 2 and HTC Vive Pro). Besides, *Omniverse Create XR* focuses on scene navigation, offering very limited support for interaction. While NVIDIA made the code of the tool available, developing extensions to support what is currently achievable in frameworks like Unity represents a huge development effort, far from what can be achieved within the scope of the project. The metaverse applications are based on extensive, diverse and multimodal interaction techniques from end-users. Adapting the Unity plugins currently used to take full advantage of XR headsets and equipment (like haptic gloves) is not achievable in the timeframe of SAFE-6G. This limitation prevented *Omniverse Create XR* from being selected as the basis for the UC1 technical architecture.

In the end, a third approach based on CloudXR and *Netcode for GameObjects* [3] was designed for UC1. Netcode for GameObjects is a high-level networking library for Unity that was made to design multiplayer applications. The factory DT app, running on a dedicated workstation, will play the role of host, managing the reference production line scene and assuring its real-time synchronization with

client applications through *Remote Procedure Calls* (RPCs). It will communicate with the metaverse manager component using TCP sockets.

The metaverse applications for the production director and line manager will play the role of clients and run on dedicated workstations. CloudXR will be used to stream video frames to their respective XR devices. For now, the envisioned XR devices are Meta Quest headsets since they are one of the only recent, video-passthrough devices compatible with CloudXR. An illustration of this architecture is available at Figure 19.

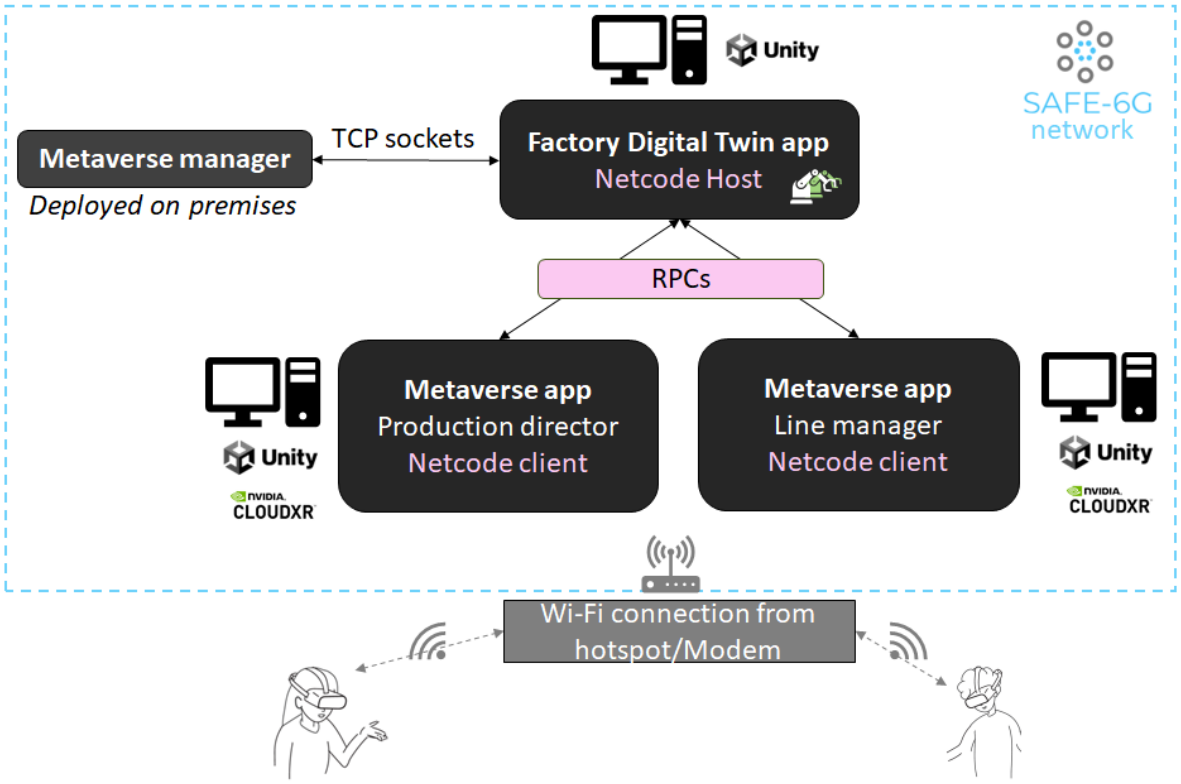

Figure 19: Technical architecture for UC1.

4.5 TECHNICAL ARCHITECTURE FOR USE-CASE 2

The main goal of the second use-case architecture is to allow the instructor to easily monitor the progress of learners. This could be achieved by letting them visualize in real-time the viewpoint of technicians to understand their progress and difficulties. To do so, the UC2 architecture is built the Shariiing suite. The ShariiingXR component from this software suite allows XR devices to stream the viewpoint of each XR headset in real-time. The resulting videos are displayed in their own dedicated thumbnail within a Shariiing session. This way, the instructor has a global common operational picture of the formation and can help technicians thanks to collaboration and guidance tools. The session runs on a dedicated workstation, allowing the instructor to work either on a traditional computer or on a large tactile screen, as illustrated in Figure 20.

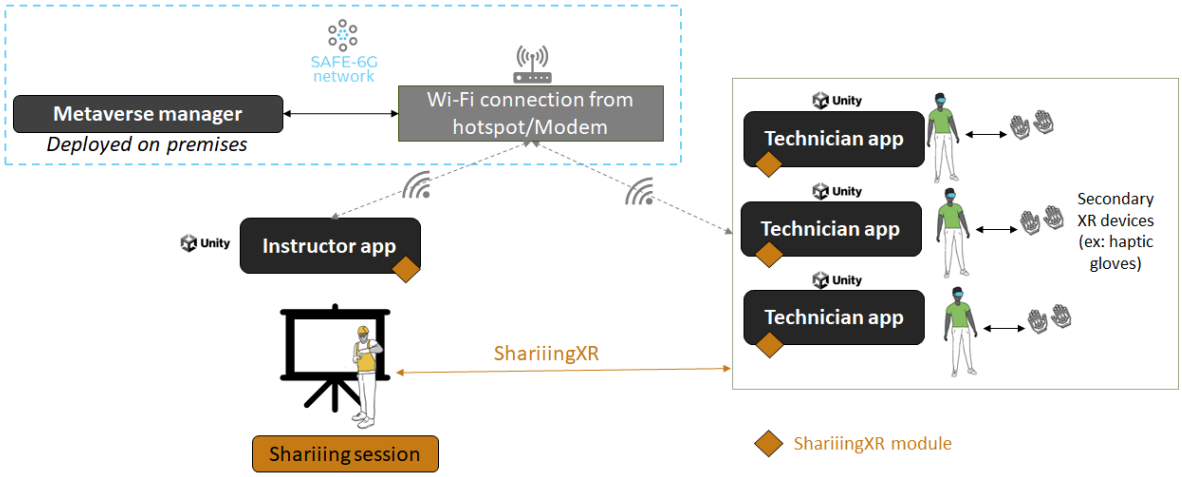

Figure 20: Technical architecture for UC2.

Each technician has its own instance of the formation application. These instances will handle the communication and synchronisation with the secondary devices like the haptic gloves for technicians. The TouchDiver [2] haptic gloves from WeArt and the Magos gloves [11] are both considered for now. The first one offers interesting thermal feedback while the latter offers better hand-tracking precision. On the instructor side, motion capture tools like the Perception Neuron [12] tracking suits are envisioned to record body postures during the initial procedure recording phase. Besides, the instructor's XR application will be the main entry point for the metaverse manager component.

5 Conclusion and Next Steps

This deliverable describes in detail the two metaverse use-cases of the SAFE-6G project. It first presents the last iteration over both use-cases scenarios, stakeholders and envisioned benefits of the approach of the project. Based on this analysis of these scenarios and stakeholders, a list of end-user's requirements, KPIs and KVIs have been proposed. Finally, a technical architecture has been designed for each use-case to clarify the involved technologies, devices and constraints.

The present document is the result of efforts conducted within the task T2.3. It will serve as reference for the end-users' perspective for SAFE-6G and as basis for the implementation work which already started in the task T3.5. The KVIs and KPIs from the system perspective will be detailed in the deliverable D2.4 - Reports on the KVI/KPI definition and validation methodology (due at Month14 – February 2025).

6 REFERENCES

[1] ‘thispersondoesnotexist.com’. Accessed: Oct. 31, 2024. [Online]. Available: https://thispersondoesnotexist.com/

[2] ‘TouchDIVER Haptic Glove | Weart’. Accessed: Nov. 14, 2024. [Online]. Available: https://weart.it/haptic-vr-products/touchdiver-haptic-glove/

[3] ‘About Netcode for GameObjects | Unity Multiplayer’. Accessed: Nov. 14, 2024. [Online]. Available: https://docs-multiplayer.unity3d.com/netcode/current/about/index.html

[4] ‘The making of VR’s most revolutionary headset’. Accessed: Nov. 14, 2024. [Online]. Available: https://garage.hp.com/us/en/innovation/revolutionary-vr-headset-hp-omnicept.html

[5] G. Wikström *et al.*, ‘What societal values will 6G address?’, May 2022, doi: 10.5281/ZENODO.6557534.

[6] ‘VIVE XR Elite - Base Station-Free PC VR in a Standalone Headset’. Accessed: Nov. 14, 2024. [Online]. Available: https://www.vive.com/us/product/vive-xr-elite/overview/

[7] ‘Meta Quest 3: New mixed reality VR headset – Shop now | Meta Store’. Accessed: Nov. 14, 2024. [Online]. Available: https://www.meta.com/fr/en/quest/quest-3/

[8] ‘NVIDIA Cloud XR’, NVIDIA. Accessed: Nov. 14, 2024. [Online]. Available: https://www.nvidia.com/en-us/design-visualization/solutions/cloud-xr/

[9] ‘USD Home — Universal Scene Description 24.11 documentation’. Accessed: Nov. 14, 2024. [Online]. Available: https://openusd.org/release/index.html

[10] ‘Omniverse Create XR — Omniverse Create XR’. Accessed: Nov. 14, 2024. [Online]. Available: https://docs.omniverse.nvidia.com/create-xr/latest/index.html

[11] ‘MAGOS Gloves - Touching the Intangible’, MAGOS. Accessed: Nov. 14, 2024. [Online]. Available: https://www.themagos.com/

[12] ‘Perception Neuron Motion Capture | Motion Capture for All’, NeuronMocap. Accessed: Nov. 14, 2024. [Online]. Available: https://neuronmocap.com/