D6.1 Project and Risk Management Plan

Security of Critical Infrastructure by Multi-Modal Dynamic Sensing and AI

01 July 2024

ITEA Project No: 22006

sintra-ai.eu

Abstract:

[Document Abstract]

Table of Contents

1 SCOPE OF THE PROJECT

Stakeholders of critical industrial and civil infrastructure, e.g., airports, harbours, power plants, construction sites, frequently suffer from the disruptions caused by an overwhelming diversity of safety and security threats. These man-made physical threats are ranging from well-organised subversive crime activities to low-level but costly actions, like vandalism, thievery, and violence. Various security monitoring and protection systems are nowadays offered on the market. The state-of-the-art SIEM solutions offer a camera network with integrated video analysis capability and video (meta)data streaming to control room operators.

However, the capabilities of these solutions are insufficient to ensure resilience and protection of critical infrastructure. Lack of trustworthy means for public-private cross-coordination, low interoperability and weak compliance with the EU data-privacy legislation are leading to local-only deployment of these systems and, as a result, fragmented situational awareness of security operators. Decisions are currently based on fragmented information within closed systems and siloed organisation models. Besides this, the common reliance on analysis of sole video data limits the monitoring to simple incidents (trespassing, panic, fighting), but does not allow detection of complex, high-impact, and context-dependent threats (human/drug trafficking, thievery, attacks on infrastructure).

The SINTRA project aims to overcome these limitations by delivering an open data-streaming AI platform that enables cross-organizational interoperability and ensures trustworthiness in the safety and security monitoring. The platform facilitates cross-coordination between involved stakeholders, aids information sharing, management, and analysis from the public and private security operators, thereby enabling global situational awareness in the infrastructure threats. SINTRA aims at researching and defining the methodology for EU legislation-aware privacy protection and ethical use of data, that serves as a basis for the cross-coordination.

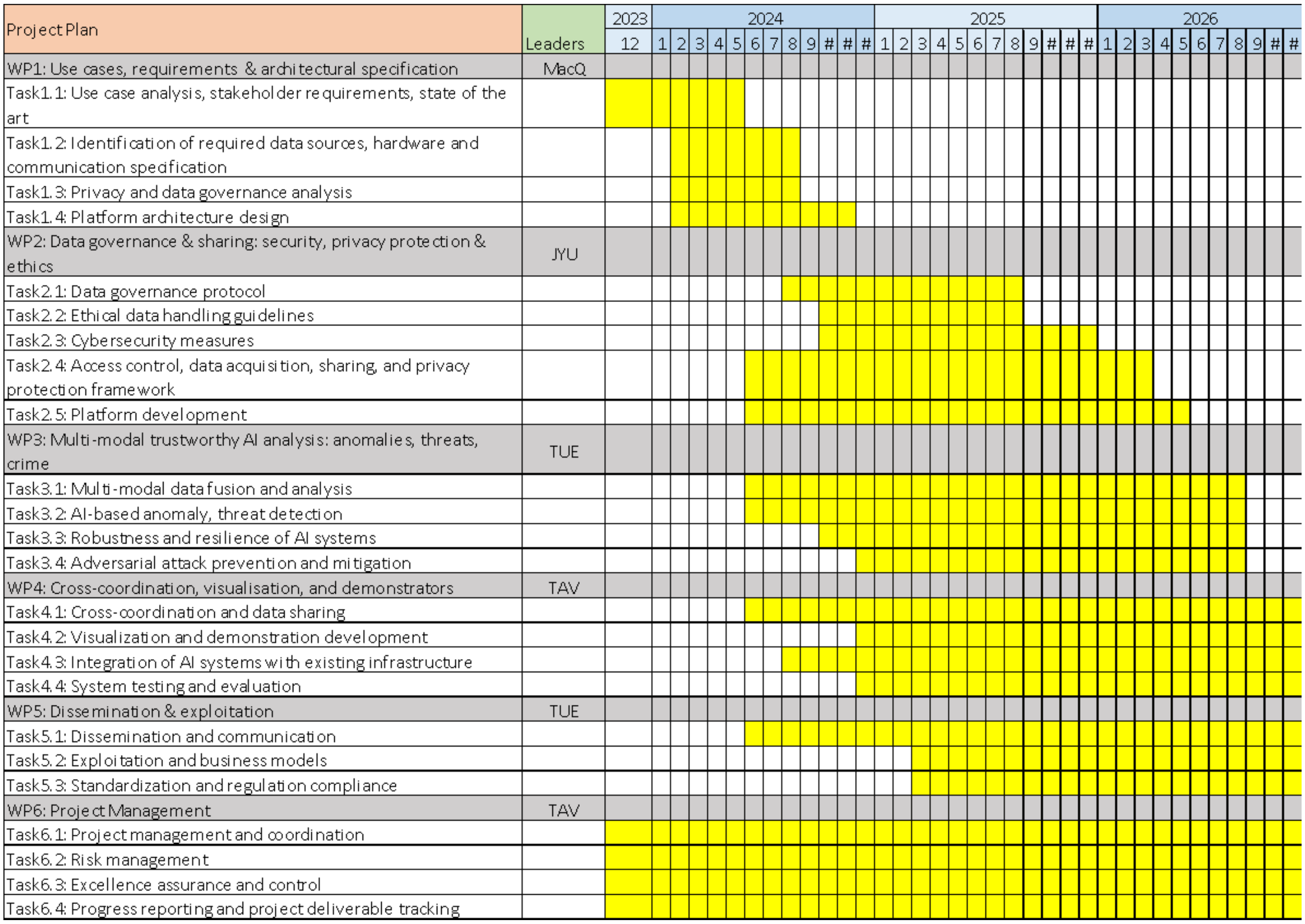
Technology-wise, the project envisions a significant step beyond the state-of-the-art by the synthesis of innovative multi-modal sensing and AI-powered combined data analysis. Incorporation and fusion of acoustic, visual, radar, multispectral, LiDAR, ToF or environmental sensor modalities together with already existing data sources (police data, logistic timetables, social media data) helps to obtain a multi-faceted, comprehensive view on the security/safety of the infrastructure situation. The AI-based analysis of the combined data enables robust detection of hidden, complex, or context-dependent anomalies, as well as their subsequent mapping to threats and timely cross-coordinated response, contingency or mitigation.

The SINTRA consortium is composed of partners from four countries (The Netherlands, Turkey, Belgium, Finland) that cover the full market value chain of research centers, sensor/data providers, platform, and service providers, where each country use-case is supported by one or more end-users. The consortium carefully balances the scale and impact of large industrial partners providing the platform and service integrations with the in-depth expertise of academic institutes and the innovative power of selected SMEs. The benefits of the SINTRA platform will be demonstrated on five critical infrastructure types of end-users: logistic hubs (Port of Moerdijk), airports (İzmir Adnan Menderes Airport), harbours, construction sites, shopping centres. The project will actively engage with citizens, authorities, and external stakeholders to stimulate acceptance, validate scalability, and maximise the impact.

The expected project business impact is threefold. First, the current analysis-based security industry is technologically stagnating due to the constantly rising legislation barriers on data collection and usage for machine learning. Establishment of the methodology for privacy-preserving AI-based security systems will enable large-scale business growth in this domain. Second, the plug-and-play SINTRA platform will help to reduce the partner maintenance and technology upgrade costs by up to 120 million euro a year. Finally, and most importantly, the project results allow partners to enter the opening market of full-fledged security and monitoring solutions, with additional revenues estimated to 400 million euro a year.

2 PROJECT PLAN

The project was initiated on December 1st, 2023 as indicated in the FPP document. The project has been planned to finish by the end of 2026.



Project Plan		2023	2024												2025												2026										
	Leaders	12	1	2	3	4	5	6	7	8	9	#	#	#	1	2	3	4	5	6	7	8	9	#	#	#	1	2	3	4	5	6	7	8	9	#	#
WP1: Use cases, requirements & architectural specification	MacQ																																				
Task1.1: Use case analysis, stakeholder requirements, state of the art		🟨	🟨	🟨	🟨	🟨	🟨																														
Task1.2: Identification of required data sources, hardware and communication specification				🟨	🟨	🟨	🟨	🟨	🟨	🟨																											
Task1.3: Privacy and data governance analysis				🟨	🟨	🟨	🟨	🟨	🟨	🟨																											
Task1.4: Platform architecture design				🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨																								
WP2: Data governance & sharing: security, privacy protection & ethics	JYU																																				
Task2.1: Data governance protocol										🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨															
Task2.2: Ethical data handling guidelines												🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨															
Task2.3: Cybersecurity measures												🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨											
Task2.4: Access control, data acquisition, sharing, and privacy protection framework								🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨								
Task2.5: Platform development								🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨						
WP3: Multi-modal trustworthy AI analysis: anomalies, threats, crime	TUE																																				
Task3.1: Multi-modal data fusion and analysis								🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨			
Task3.2: AI-based anomaly, threat detection								🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨			
Task3.3: Robustness and resilience of AI systems												🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨			
Task3.4: Adversarial attack prevention and mitigation														🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨			
WP4: Cross-coordination, visualisation, and demonstrators	TAV																																				
Task4.1: Cross-coordination and data sharing								🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task4.2: Visualization and demonstration development														🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task4.3: Integration of AI systems with existing infrastructure										🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task4.4: System testing and evaluation														🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
WP5: Dissemination & exploitation	TUE																																				
Task5.1: Dissemination and communication								🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task5.2: Exploitation and business models																	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task5.3: Standardization and regulation compliance																	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
WP6: Project Management	TAV																																				
Task6.1: Project management and coordination		🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task6.2: Risk management		🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task6.3: Excellence assurance and control		🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
Task6.4: Progress reporting and project deliverable tracking		🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨

Figure 1. Project Plan

3 PROJECT WORK PACKAGES

The project is structured into six distinct sections as depicted in the following figure. Work Package 1 (WP1) is dedicated to outlining the use cases, stakeholder requirements and establishing the architectural design of the SINTRA project. Following WP1, Work Package 2 (WP2) takes charge of data governance, ethical data handling guidelines, cybersecurity measures, data privacy and ethics. Work Package 3 (WP3) is a phase of intense research and development, focusing on crafting technological solutions that address both specific and overarching issues within the system. The process during WP3 will be dynamic, adopting an iterative and agile approach. In that work package, a multi-modal trustworthy AI analysis will be carried out. Upon the completion of WP3, Work Package 4 (WP4) steps into implementing the identified business scenarios on the technological infrastructure.

Throughout these stages, the progress and outputs from WP1, WP2, WP3 and WP4 are regularly shared with Work Package 6 (WP6). Meanwhile, Work Package 5 (WP5) leverages the outputs from all preceding work packages to engage in dissemination and exploitation activities. Moreover, WP6 plays a crucial role in orchestrating the coordination among all work packages, ensuring the project progresses smoothly and achieves its set objectives.

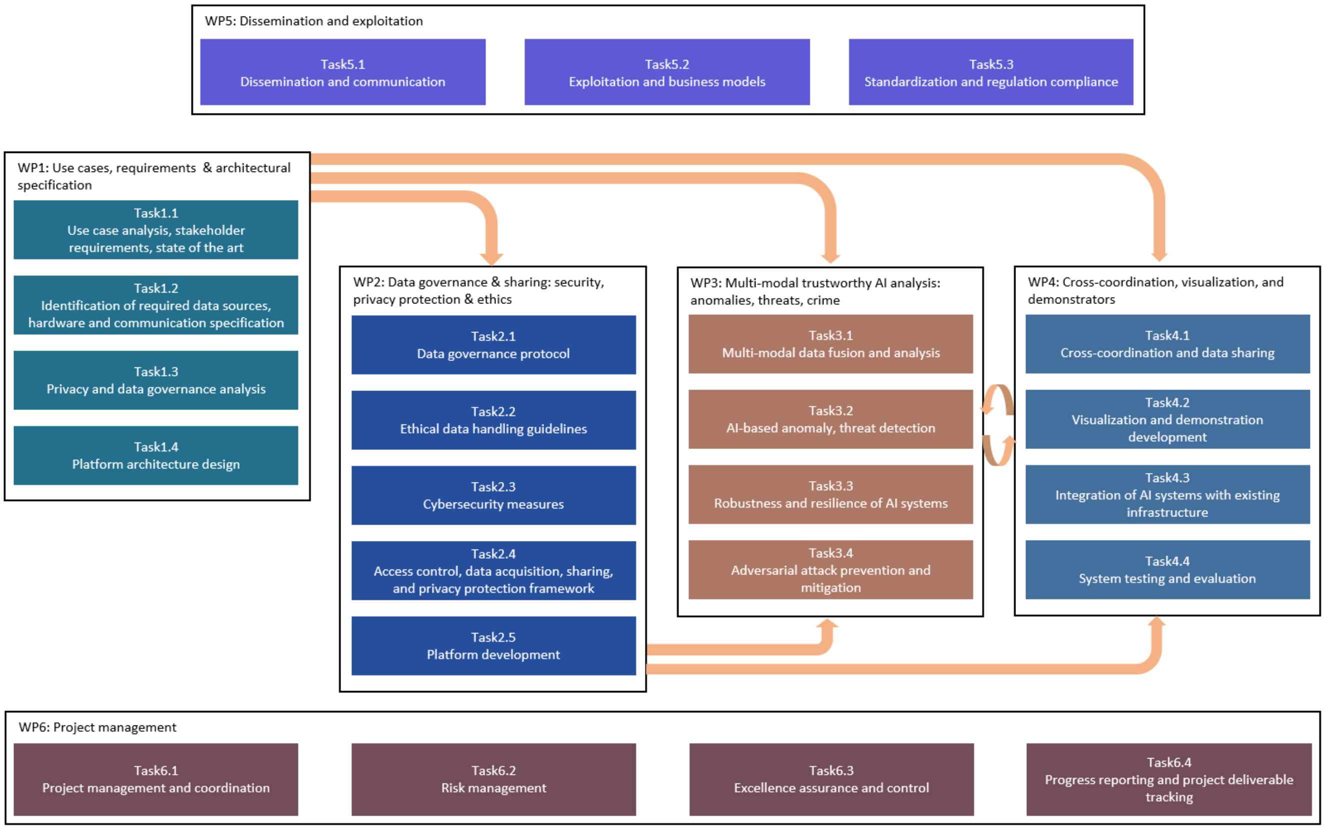

WP5: Dissemination and exploitation
Task5.1 Dissemination and communication
Task5.2 Exploitation and business models
Task5.3 Standardization and regulation compliance
WP1: Use cases, requirements & architectural specification
Task1.1 Use case analysis, stakeholder requirements, state of the art
Task1.2 Identification of required data sources, hardware and communication specification
Task1.3 Privacy and data governance analysis
Task1.4 Platform architecture design
WP2: Data governance & sharing: security, privacy protection & ethics
Task2.1 Data governance protocol
Task2.2 Ethical data handling guidelines
Task2.3 Cybersecurity measures
Task2.4 Access control, data acquisition, sharing, and privacy protection framework
Task2.5 Platform development
WP3: Multi-modal trustworthy AI analysis: anomalies, threats, crime
Task3.1 Multi-modal data fusion and analysis
Task3.2 AI-based anomaly, threat detection
Task3.3 Robustness and resilience of AI systems
Task3.4 Adversarial attack prevention and mitigation
WP4: Cross-coordination, visualization, and demonstrators
Task4.1 Cross-coordination and data sharing
Task4.2 Visualization and demonstration development
Task4.3 Integration of AI systems with existing infrastructure
Task4.4 System testing and evaluation
WP6: Project management
Task6.1 Project management and coordination
Task6.2 Risk management
Task6.3 Excellence assurance and control
Task6.4 Progress reporting and project deliverable tracking

Figure 2. Work Packages

The organizational and management framework of the SINTRA project is detailed in the following table. As seen from the table the project is a large-scaled one with respect to the number of partners from four countries. Designed to align with the project's scale and intricacy, this structure includes:

Project Coordinator (PC): Gökhan Koç (TAV Technologies)

Country Coordinators (CC): Gökhan Koç (TAV Technologies - Turkey), Dr. Egor Bodarev (Eindhoven University of Technology - Netherlands), Anna Hristoskova (Sirris – Belgium), Markus Sihvonen (University of Jyväskylä – Finland)

Work Package Leaders (WPL):

- WP1: Geert Vanstraelen (MACQ)
- WP2: Dr. Markus Sihvonen (University of Jyväskylä)
- WP3: Dr. Egor Bodarev (Eindhoven University of Technology)
- WP4: Gökhan Koç (TAV Technologies)
- WP5: Dr. Egor Bodarev (Eindhoven University of Technology)
- WP6: Gökhan Koç (TAV Technologies)

A Project Management Team (PMT): The PMT is responsible for the overarching, ongoing management of the project. This team is composed of the Project Coordinator (PC), Work Package Leaders (WPL), Country Coordinators (CC), and representatives from each partnering organisation.

Table 1. Project Management Team

Full Name	Organization	Country	Email Address
Gökhan Koç	TAV Tech	TR	Gokhan.Koc@tav.aero
Dr. Egor Bodarev	Eindhoven University of Technology	NED	e.bondarev@tue.nl
Anna Hristoskova	Sirris	BEL	anna.hristoskova@sirris.be
Dr. Markus Sihvonen	University of Jyväskylä	FIN	markus.v.sihvonen@jyu.fi
Geert Vanstraelen	MacQ	BEL	Geert.Vanstraelen@macq.eu
Dr. İsmail Uzun	Inosens	TR	ismail.uzun@inosens.com.tr
Gözde Sayın	TAV Tech	TR	gozde.sayin@tav.aero
Dr. Seçil Heper	TAV Tech	TR	secil.heper@tav.aero
Prof. Tapio Frantti	University of Jyväskylä	FIN	tapio.k.frantti@jyu.fi

4 PROJECT MANAGEMENT METHODOLOGY

A dedicated channel on Microsoft Teams has been established as the primary workspace for the project. This channel serves as the central hub for all communications, data storage, and other collaborative needs.

A steering committee, comprising representatives from various institutions, has been formed for the project. Each member of the monitoring committee, representing both individual and institutional stakeholders, has been thoroughly briefed on the project's intricacies. To ensure they can effectively follow the project's progress, they have been added as members of the Microsoft Teams channel.

Regular weekly meetings are convened involving all members of the consortium. These meetings serve to review the project's progress, address any issues, and ensure that all parties are aligned and informed about the current status and next steps.

To streamline communication and collaboration, contact information for all partners associated with the project has been meticulously compiled and integrated into an email contact list. This initiative enables various departments, including legal, operations, and others, to communicate directly and efficiently without necessarily requiring the mediation of the project coordinator.

The project coordinator, TAV Technologies, plays a pivotal role in facilitating communication and understanding among the stakeholders. They periodically organise meetings, bringing together partners and airport operation managers. These meetings are instrumental in clarifying requirements, discussing expectations, and ensuring that the needs and objectives of all parties are fully understood and addressed.

5 QUALITY & RISK MANAGEMENT COMMITTEE

During the project and afterward, to manage the process related to risks that may arise, the project management team has established a risk and quality monitoring and management committee consisting of representatives from various partners within the consortium, as indicated in the figure below.

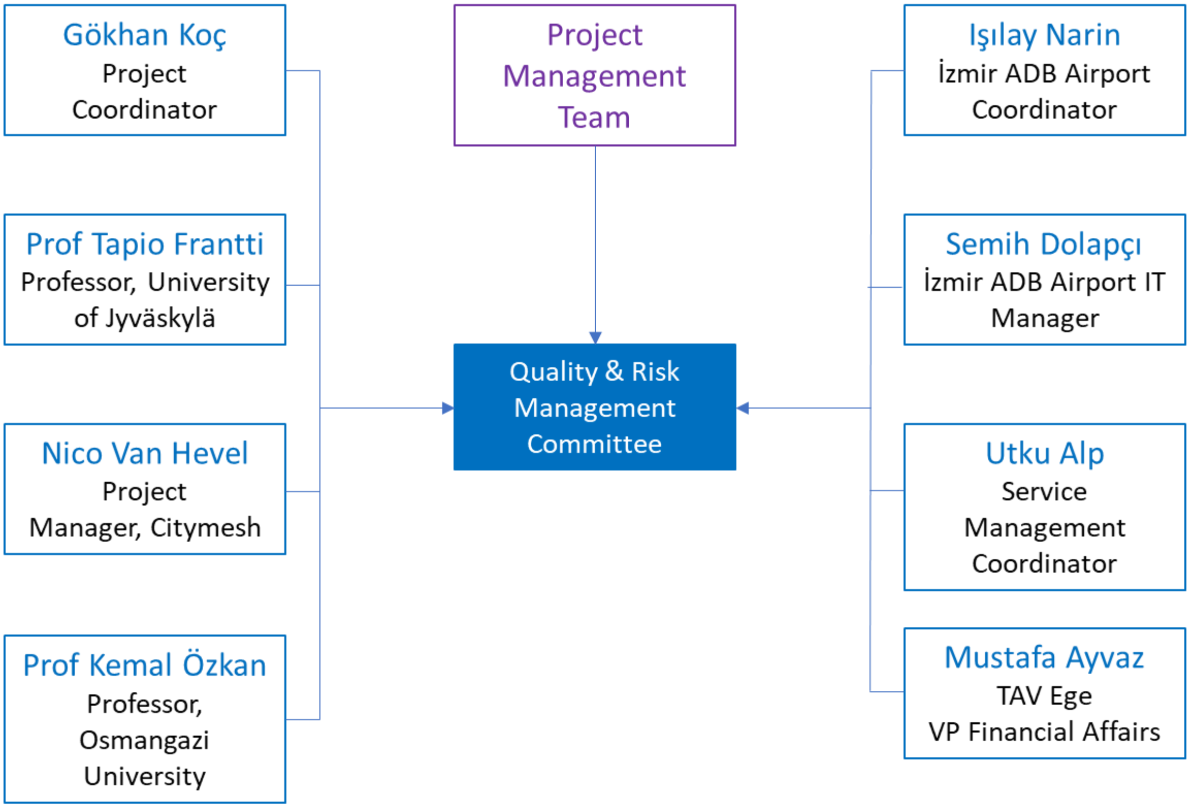

Gökhan Koç
Project Coordinator
Prof Tapio Frantti
Professor, University of Jyväskylä
Nico Van Hevel
Project Manager, Citymesh
Prof Kemal Özkan
Professor, Osmangazi University
Project Management Team
Quality & Risk Management Committee
Işılay Narin
İzmir ADB Airport Coordinator
Semih Dolapçı
İzmir ADB Airport IT Manager
Utku Alp
Service Management Coordinator
Mustafa Ayvaz
TAV Ege
VP Financial Affairs

Figure 3. Quality & Risk Management Committee

Every individual contributes significantly to the Quality and Risk Management Committee, utilising their specialised skills to guide the project towards its objectives. As the Project Coordinator, Gökhan Koç is at the helm, orchestrating the project's progression in harmony with its goals and schedules, fostering team synergy, and acting as the primary liaison for all communications.

Additionally, the project managers from all partner companies will also be members of the Quality and Risk Management Committee.

6 RISK MANAGEMENT PROCESS

6.1 Regular Committee Meetings

The Quality and Risk Management Committee will hold meetings for each 3-months to supervise and direct the project's quality and risk-related activities. These meetings are crucial for addressing current and emerging issues, evaluating the progress of the project, and making informed decisions regarding quality and risk.

6.2 Role of the Project Manager

The Project Manager is tasked with organising these committee meetings. Responsibilities include preparing the agenda, informing members about the meeting details, ensuring all necessary documents are ready, and leading the discussions. The Project Manager serves as a bridge, ensuring that the committee's decisions and plans are well communicated and executed by the project team.

6.3 Deliverable Approval Process

The committee is responsible for approving all project outputs. This involves a detailed inspection to confirm that each output adheres to the set quality criteria and is free from significant risks. Gaining the committee's approval means the output has met all requirements and is ready for either the next project phase or delivery to the client.

6.4 Maintaining Documentation

It's essential to record all decisions, risk evaluations, and quality checks. This documentation captures the essence of each meeting and serves as an accountability and reference tool for future needs

6.5 Ongoing Enhancement

The committee is committed to continual enhancement, learning from each project stage to refine future processes and results. This means consistently updating our approaches to risk management and quality criteria to incorporate new findings and adapt to the evolving nature of the project.

7 RISK & ACTION LIST

Following risks are defined by the Quality and Risk Management Committee. List will be alive during the project.

No	Risk	Action	Probability (P)*	Severity (S)**	Impact (PxS)***	Status
1	**Data Privacy and Security Risks** The integration of various systems and the handling of sensitive data, especially in an airport and in harbour setting, could lead to data breaches or unauthorized access if not properly secured.	… security team will develop the best network architecture to eliminate risks defined.	**3**	**2**	**6**	**Active**
2	**Regulatory Compliance Risks** With operations potentially spanning multiple countries, the project could face challenges in complying with various local, national, and international regulations, especially concerning data protection (like GDPR).	Airport operation managers, harbour operation managers, TAV Tech Aviation academic consultant, … will guide the project team about the regulations.	**2**	**3**	**6**	**Active**
3	**Technology Integration and Interoperability Risks** The SINTRA platform involves integrating multiple technologies and systems. There's a risk that these systems may not integrate smoothly, leading to inefficiencies or failures.	Preliminary feasibility studies have been conducted and no issues have been observed.	**3**	**1**	**3**	**Active**
4	**Vendor Lock-in Risks** The project seems to rely on certain technologies and vendors. There could be a risk of vendor lock-in, making it difficult or costly to switch vendors in the future if needed.	All hardware components will be selected from those with numerous alternatives, and the hardware layer will be abstracted in all studies.	**2**	**3**	**6**	**Active**

5	**Scalability and Performance Risks** As the system scales, there might be unforeseen challenges related to the performance of the integrated systems, especially under high load or during rapid scaling events.	Will be considered in platform architecture design work	**4**	**3**	**12**	**Active**
6	**Dependency on Open Source Tools Risks** While using open source tools can be beneficial, it also comes with risks such as lack of support, unexpected changes or discontinuation of the tools, and potential security vulnerabilities.	Alternatives for open source solutions will be determined in the platform architecture design study.	**1**	**4**	**4**	**Active**
7	**Change Management and Training Risks** There's a risk that staff may not be adequately trained or resistant to change, leading to a failure in adopting the new system.	Agile methodologies will be applied in all project development processes, and change will exist as a necessity of the job.	**2**	**1**	**2**	**Active**
8	**Project Management and Coordination Risks** Given the project's scope and the number of stakeholders involved, there's a risk of miscommunication, misalignment of goals, or delays due to poor project management or coordination.	Each partner in the project has designated 1 project manager, and the project is carried out with the relevant resources. On the other hand, entire process will be documented to not lose any detail or to not create a misunderstanding situation.	**3**	**2**	**6**	**Active**
9	**Cost Overruns and Budgeting Risks** Complex projects like SINTRA often face the risk of exceeding initial cost estimates. Unexpected expenses can arise from technical hurdles, extended timelines, or changes in project scope.	Efficiency will be maintained at the highest level with agile methodologies.	**2**	**2**	**4**	**Active**
10	**System Reliability and Uptime Risks**	During the research phase, it is not a	**4**	**4**	**16**	**Active**

	Ensuring the high availability and reliability of the SINTRA platform is crucial, especially in an airport and harbour setting where downtime can lead to significant operational disruptions.	requirement for the system to remain live 24/7. However, after the project is completed, such a need will arise, and the infrastructure preparedness related to redundancy will be carried out during the project process.				
11	**Legal and Ethical Risks** The use of AI and data analytics in sensitive areas such as airports and harbours raise legal and ethical concerns, including issues related to passenger privacy, data usage consent, and the ethical implications of AI decisions.	Airport operation managers, harbour operation managers, TAV Tech Aviation academic consultant, … will guide the project team about the regulations.	**2**	**3**	**6**	**Active**
12	**Intellectual Property Risks** In a project involving multiple partners and possibly open-source tools, there's a risk related to the proper management and protection of intellectual property rights.	Detailed IP sharing protocol is defined and will be approved by all parties in the PCA document when signed.	**1**	**1**	**1**	**Active**
13	**End-User Adoption and Usability Risks** The success of the SINTRA platform heavily depends on its adoption by end-users. There's a risk that the platform may not be user-friendly or meet the specific needs of its users, leading to low adoption rates and underutilization.	Potential users of SINTRA are already inserted in steering committee and they will guide development teams and increase usability.	**1**	**3**	**3**	**Active**
14	**Accuracy and Precision of AI Predictions** The effectiveness of the SINTRA platform relies on the accuracy of its AI and ML predictions. Incorrect or imprecise predictions	Will be considered in partner solutions architectures design work.	**3**	**3**	**9**	**Active**

	can lead to operational inefficiencies, safety issues, or negative customer experiences.					
15	**Incident Response and Recovery Risks** In the event of a system failure or security breach, the ability of the SINTRA platform to quickly respond and recover is crucial. Inadequate incident response mechanisms can exacerbate the impact of such events.	Will be considered in platform architecture design work	**1**	**4**	**4**	**Active**

*: 5 denotes Frequent; 4 Occasional; 3 Remote; 2 Improbable; 1 Extremely improbable.

**: 5 denotes Catastrophic; 4 Hazardous; 3 Major; 2 Minor; 1 Negligible

***: Risk impact is calculated by multiplying probability with severity. The results which are equal or bigger than 15 are of major concern. The results between 4 and 15 are of concern. The results which are equal or smaller than 4 are negligible.