# Project Progress Report Annex

Version 24, December 2024

# Foreword

*Do not remove or modify in any way the sections having these notations.*

*All guidelines in the template appear in this "boxed" format. These instructions, as well as the preceding title page ("PPR Annex template") and this foreword, should never be removed manually from the submitted files as they are automatically removed by the merging function of the ITEA Community website.*

*It is highly recommended that you carefully read all the instructions provided: they indicate for each chapter and subchapter what is expected and must be carefully considered.*

*It is crucial that you comply with the pre-defined formatting and styling rules: breaking these rules may create errors when inserting the auto-generated sections and thus cause the merge process to fail. Complying with formatting rules can be achieved by adhering to the following guidelines:*

- *do not remove any predefined titles and do not add headers, incl. Annexes.*

*do not modify the predefined styles, except for standard "emphasis" effects (i.e., underlined, or bold text). We recommend you use underlining and bolding in a consistent and prudent way throughout the document, and on body text exclusively.*

- *only use the pre-defined styles.*
- *do not remove the instructions (both green and orange ones), and do not remove the auto-generated sections.*
- *do not overload the document with uncompressed / excessively large images, a report should ideally fit in less than 10 MB.*

*Potential layout issues that appear when the instructions are removed will be adjusted by the ITEA Office, between the report submission and the transfer of the generated PPR to the reviewers.*

*It is in the interest of the consortia to ensure that a merged document (i.e., including auto-generated sections) can be generated and downloaded before the submission deadline, so that all the relevant information is provided in the Project Progress Report.*

This red text box is an indicator of the auto-generated sections.
Do not remove or modify in any way the sections having these notations throughout the whole Annex template since they are needed to automatically merge the information provided via the ITEA Community website with your uploaded Annex document.

# 2024-H2 Project Progress report

## SINTRA

SECURITY OF CRITICAL INFRASTRUCTURE USING MULTI-SENSOR AND DYNAMIC ARTIFICIAL INTELLIGENCE

Edited by: All Consortium Partners

Date: March 17, 2025

## Project key data

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

The inserted key data will contain (among others) acronym, full title, time frame, the respective countries and partners per country, the coordinator, project status as well as the PCA status.

## Project Acronyms

| | |
|---|---|
| AI | Artificial Intelligence |
| CCTV | Closed-Circuit Television |
| EU | European Union |
| F&B | Food &Beverage |
| GDPR | General Data Protection Regulation |
| IoT | Internet of Things |
| KPI | Key Performance Indicator |
| mmWave | millimetre-Wave |
| RF | Radio Frequency |
| SINTRA | Security of Critical Infrastructure by Multi-Modal Dynamic Sensing and Artificial Intelligence |
| VR | Virtual Reality |
| WP | Work Package |
| | |
| | |
| | |
| | |

# Table of contents

# 1. Project one-page description

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

# 2. Project overall status

## 2.1. Top 4 overall targeted innovations

*Select the top 4 targeted innovations for the whole project, i.e., the main innovative results the project aims to achieve before its closure. Avoid generic terms, remain brief and to the point, by focusing on what the project really brings new to the table.*

*For each targeted innovation, please indicate:*

- *the main contributors (only the key contributors are expected there, not an exhaustive list of all contributors).*

*a short description and the current State-of-the-Art related to the proposed innovation. The provided descriptions should be detailed enough to be self-explanatory, approximately in 50-100 words per innovation.*

*Please note that innovations are not necessarily deliverables per se.*

**1. AI-Powered Anomaly Detection & Security Threat Identification**

***Main contributors***: All partners

***Short description of innovation and the State-of-the-Art***:

SINTRA integrates advanced AI models for anomaly detection using multi-modal data from cameras, IoT sensors, RF signals, and mmWave radars. AI techniques, including deep learning and video analytics, enhance security by identifying threats such as unauthorized access, violence, and cyber risks in airports, ports, and critical infrastructures. The system ensures real-time monitoring with automatic alerts, improving situational awareness and rapid response. Innovations in privacy-preserving AI and federated learning also enable secure data processing while maintaining compliance with GDPR and ethical AI principles. This technology significantly improves security monitoring across diverse, high-risk environments.

**2. Multi-Tenant, Scalable AI Infrastructure for Smart Surveillance**

***Main contributors***: All partners

***Short description of innovation and the State-of-the-Art***:

The SINTRA platform offers a scalable, AI-driven solution built on technologies like Kafka, ClickHouse, Kubernetes, and NVIDIA DeepStream. Designed for real-time security monitoring in dynamic environments, it enables seamless integration with partner systems, supporting multi-tenancy and edge computing. The infrastructure processes high-FPS camera streams, IoT data, and sensor inputs for predictive analytics and anomaly detection. Secure access control through Keycloak and TLS encryption ensures data integrity and privacy. By leveraging AI-powered threat detection and

decentralized computing, the platform enhances operational efficiency while maintaining compliance with cybersecurity and regulatory standards across multiple industries.

**3. IoT-Driven Smart Sensing & Situational Awareness**

***Main contributors***: All partners

***Short description of innovation and the State-of-the-Art***:

SINTRA leverages IoT-enabled smart sensing to enhance situational awareness in airports, ports, and construction sites. By integrating data from cameras, vibrations, RF signals, BLE sensors, and mmWave radars, the system enables precise object detection, people tracking, and risk assessment. The fusion of multimodal sensor data provides a comprehensive security landscape, reducing false alarms and improving response accuracy. Advanced analytics enable real-time data processing on edge devices, ensuring rapid decision-making. With robust cybersecurity measures and privacy-aware data handling, the innovation provides an intelligent, connected environment for enhanced safety, efficiency, and automation in high-risk infrastructures.

**4. Privacy-Preserving AI & Secure Data Governance**

***Main contributors***: All partners

***Short description of innovation and the State-of-the-Art***:

The project pioneers privacy-preserving AI techniques, including image anonymization, fragile watermarking, and federated learning, ensuring ethical AI deployment. Secure data governance models incorporate access control policies, encryption, and GDPR compliance, allowing multi-stakeholder collaboration without compromising privacy. AI-driven data masking techniques ensure that personally identifiable information (PII) is protected while retaining the analytical value of the data. Additionally, federated AI training across distributed edge and cloud environments minimizes centralized data storage risks. By implementing zero-trust security models and blockchain-based audit trails, SINTRA ensures the integrity, confidentiality, and reliability of AI-powered surveillance and security solutions.

*Copy the above template if more targeted innovations need to be indicated.*

## 2.2. Top 4 overall targeted business impacts

*Select the top 4 targeted business impacts for the whole project, i.e., the main business results the project aims to achieve by and after project closure. Avoid generic terms, remain brief and to the point, by focusing on what the project expects to achieve business-wise thanks to the project's technical results.*

*For each targeted business impact, please indicate:*
*a short description of the business impact.*

- *the main contributors (only the key contributors are expected there, not an exhaustive list of all contributors), and*

*the targeted market and its current competitors, approximately in 50-100 words.*

**1. Security and Anomaly Detection at Airports**

***Short description***: The project will introduce AI-driven anomaly detection to improve security at airports. By integrating multi-modal data from cameras, IoT sensors, RF signals, and audio sources, the system can proactively identify threats such as unauthorized access, unattended baggage, and suspicious behavior. Real-time alerts will enable swift intervention, reducing security breaches and operational disruptions.

***Main contributors***: TAV Technologies, Koçsistem, Alpata

***Market / competitors***:

The primary market includes international and regional airports, aviation security agencies, and government regulatory bodies. As global air travel rebounds, demand for AI-powered security solutions is rising, making airports key adopters. Established players such as Thales, SITA, and Honeywell offer security solutions, but few integrate real-time AI-powered multi-sensor detection. The SINTRA Airport Platform aims to provide a scalable, high-precision alternative with enhanced threat recognition capabilities.

**2. AI-Powered F&B Safety and Surveillance**

***Short description***: The introduction of AI-based food safety monitoring in airport food and beverage (F&B) areas will enhance compliance with hygiene regulations and detect potential security risks. AI models will monitor food handling, hygiene practices, and even detect unusual activities such as contamination or tampering in real time.

***Main contributors***: Koçtaş, İnosens, ARD

***Market / competitors***:

The market includes airport F&B vendors, regulatory agencies, and global catering companies. With increasing food safety concerns and regulatory scrutiny, airports are seeking smarter, automated compliance solutions. Companies such as NEC and Bosch provide AI-driven surveillance, but dedicated AI solutions for F&B safety are limited. This project aims to differentiate itself by offering a solution specifically optimized for the high-traffic, time-sensitive nature of airport F&B operations.

**3. Security and Compliance Across Critical Infrastructure**

***Short description***: The SINTRA project delivers cutting-edge AI-driven security and compliance solutions for airports, ports, construction sites, and rail networks. By integrating advanced sensor

fusion, real-time video analytics, and secure data governance, the platform ensures proactive threat detection, privacy compliance, and operational integrity. With features like AI-powered anomaly detection, automated access control, and federated learning for ethical AI, SINTRA strengthens resilience against security threats while maintaining regulatory compliance, such as GDPR. These innovations support safer environments, reducing unauthorized access, improving situational awareness, and enhancing crisis response capabilities across industries.

***Main contributors***: All partners

***Market / competitors***:

The market includes municipalities, law enforcement agencies, and urban planning organizations. With cities worldwide embracing AI for safety and operational efficiency, there is a growing demand for solutions that balance security with privacy protection. Traditional surveillance companies like Motorola Solutions and Dahua focus on AI-based monitoring, but privacy-preserving AI solutions remain a niche. The SINTRA project aims to position itself as a leader in ethical AI for public safety.

**4. AI Driven Surveillance for Critical Infrastructure**

***Short description***: AI-based monitoring solutions will be implemented in ports, railway stations, and construction sites to detect unauthorized access, hazardous activities, and potential cyber threats. Combining AI-powered video surveillance, mmWave radar sensing, and automated risk assessment will enhance the security of critical infrastructures.

***Main contributors***: All partners

***Market / competitors***:

Governments, private infrastructure companies, and security service providers will benefit from this technology. The increasing need for infrastructure protection against physical and cyber threats is driving investments in smart surveillance solutions. Companies such as Hikvision, Axis Communications, and Genetec provide security monitoring, but integrating multi-modal AI analysis (thermal, video, RF signals) in a real-time decision-making system provides a unique value proposition.

*Copy the above template if more targeted business impacts need to be indicated.*

## 2.3. Top 4 overall project KPIs

*This section relates to the FPP chapter "Quantified objectives and quantification criteria". Elaborate the Key Performance Indicators (KPIs) as mentioned in the FPP considering the expected main project results, ie., the "Top 4 targeted innovations" and the "Top 4 targeted business impacts" mentioned above in this PPR. The KPIs must quantify these expected project*

*results and allow both the consortium and the evaluators to monitor the progress of each of them towards the goals.*

*The KPIs section refers to the project's final goals (not strictly to the reporting period) and are thus presumably quite stable from one PPR to the next one (except for the current status update). In the lifetime of an ITEA project, the actual project goals may, however, be refined or slightly reoriented (e.g. to adapt to changes in the technological State-of-the-Art or in the market environment): in such cases, the project may update its KPIs if needed, so that they fit with the new adapted goals.*

*In the Project Progress Report, project management related KPIs (such as the number of milestones completed in time) should be excluded.*

*For each defined KPI, please indicate:*

- *the status of KPI in the beginning of the project (Initial value);*

*the targeted value, computed thanks to the defined metric (whenever possible, provide the unit of measurement, e.g. "%", "ms" or "fps");*

- *the current value, and*
- *the metric description, i.e. how the actual values are computed, incl. the reference architecture / hardware / algorithm / data, whenever relevant.*

| | Initial value | Targeted value | Current value |
|---|---|---|---|
| **1.Threat detection success of CCTV Analyzer compared to alternatives** | - | min 95% | 100% (continuous monitoring) |

A version of the system that works synchronously with a few cameras will be prepared and comparisons will be made with this version.

| | | | |
|---|---|---|---|
| **2. IoT AI-based fraud detection accuracy in airport shops** | - | min 0.85 (F-Score) | 0.89 achieved in more simple case |

Event records kept by security teams at the airport will be compared with system outputs.

| | | | |
|---|---|---|---|
| **3. Amount of detectable complex crime-related anomalies** | - | 7 public safety threats. | Current: 0/2 (violence and object throwing) |

3 anomaly types: drugs trafficking, people smuggling and cargo thievery. Actors physically play the anomalies in the field lab of Port of Moerdijk, and the detection results are assessed.

| | | | |
|---|---|---|---|
| **4. GDPR compliance while linking multiple data streams** | - | Adhere to GDPR Rules | No comparable current rate in literature |

Camera streams from multiple sites will be combined along with external information sources to validation algorithm compliance.

*Copy the above template if more result KPIs need to be indicated.*

## 2.4. Top 4 overall risks

*Analyse any possible risks (technological, managerial, commercial, etc.) identified during the reporting period.*

*Identify the top 4 risks for the project, and for each of them, present ideally both:*
*an appropriate and realistic avoidance action;*
*an appropriate mitigation / back-up plan, in case the realisation of the risk cannot be avoided, approximately in 30-50 words per risks, and*

- *a period in which the risk is relevant (e.g. end of the project).*

*The analysis of the commercial risks is crucial during a project's final year (and recommended for previous years).*

*For each risk, define also its **Severity** and **Probability** of occurrence.*

**Severity** is indicated as one of the following:
*Low: the impact on the project would be minimum and easily repairable (e.g. a partner is leaving and its tasks can mostly be transferred to remaining partners).*
*Medium: the project would be impacted, but the core project outcomes, despite being somehow downsized, would remain very relevant (e.g. the technological breakthrough is not fully achieved, with performances 20% below what was planned, while remaining above the State-of-the-Art).*
*High: the project would be significantly impacted, with a considerably decreased business impact (e.g. one of the three core partners for the exploitation reshapes its strategic planning and decides to leave the targeted market).*
*Critical: the rationale of the project would be at stake, and a complete reshaping of the future goals would be required (e.g. a competitor markets a product comparable to what was planned, two years before the project planned delivery).*

***Probability** of occurrence is indicated as:*

- *Rare: 1-10 % of chance to occur.*

- *Possible: 10-50 % of chance to occur.*
- *Likely: 50- 90 % of chance to occur.*
- *Almost certain: ≥ 90 % of chance to occur.*

***Stage** of each risk should be indicated too:*
*Identifying: A risk has been identified and the project consortium is developing avoidance action or back-up plan.*

- *Mitigating: The consortium is applying avoidance actions or implementing back-up / mitigation planning*
- *Monitoring & Controlling: The risk is under control.*

| | Severity | Probability | Stage |
|---|---|---|---|
| **1. Data Privacy and Security Risks** | Medium | Likely | Mitigating |

***Avoidance action***:

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. Legal experts are to be engaged early in the process to ensure full compliance with GDPR and other relevant privacy regulations. Regular audits of data handling processes should be performed.

***Back-up / Mitigation plan***:

Security team will develop the best network architecture to eliminate risks defined. If compliance issues arise, anonymization and encryption techniques are to be prioritized to ensure privacy. Working closely with regulators and modifying processes as needed to ensure legal compliance is required before the product goes live.

***A period in which the risk is relevant***

Final stages and at the time of market release.

| | | | |
|---|---|---|---|
| **2. Regulatory Compliance Risks** | High | Possible | Mitigating |

***Avoidance action***:

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). Legal experts are to be engaged early in the process to ensure full compliance with GDPR and other relevant privacy regulations. Regular audits of data handling processes should be performed.

***Back-up / Mitigation plan***:

Airport operation managers, harbour operation managers, TAV Tech Aviation academic consultants will guide the project team about the regulations.

***A period in which the risk is relevant***

Final stages and at the time of market release.

| | | | |
|---|---|---|---|
| **3. Technology Integration and Interoperability Risks** | High | Possible | Monitoring & Controlling |

***Avoidance action***:

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.

***Back-up / Mitigation plan***:

Additional resources to ensure smooth integration of multi-modal sensors and hardware components are to be allocated. Modular hardware and early-stage prototype testing are to be used to detect integration issues early on.

***A period in which the risk is relevant***

Mid to late stages of the project, especially before deployment.

| | | | |
|---|---|---|---|
| **4. Vendor Lock-in Risks** | High | Possible | Monitoring & Controlling |

***Avoidance action***:

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.

***Back-up / Mitigation plan***:

All hardware components will be selected from those with numerous alternatives, and the hardware layer will be abstracted in all studies.

***A period in which the risk is relevant***

Mid to late stages of the project, especially before deployment.

*Copy above template if more risks need to be indicated.*

## 2.5. Change in the technology and market during the reporting period

*Reconsider the relevance, importance and impact of the project with respect to the current technological State-of-the-Art (as opposed to the one described in the FPP) and to the current*

*and forecasted trends. Address possible new or similar projects. Also document the market relevance changes that occurred since the PPR was issued.*

*Do not refer the changes in technology and business within your project but report the changes in the "external world". Do not copy technical and strategic relevance related sections from previous PPRs, only report on updates and evolutions. If major changes occurred since the latest PPR or FPP release, document such changes in this paragraph. If the technological and business relevance has not changed, state it here.*

Technological Evolution

During the 2nd semester of 2024, the external technological landscape has experienced little change that will have effect on SINTRA project. The rise of GenAI tools and the introduction of meta-models are reshaping the AI driven solution in critical infrastructure projects. In 2024, there has been a notable expansion of AI projects focusing on critical infrastructure protection, driven by regulatory pressures and increasing concerns over cybersecurity and physical safety. The competition has grown, with projects in areas such as smart cities, transport hubs, and industrial facilities employing similar technologies. Additionally, the need for AI systems capable of real-time analysis, such as SINTRA, is becoming even more critical as infrastructures move toward automation and digitization.

With stricter data privacy regulations (e.g., GDPR updates, AI Act in the EU, and NIST AI Risk Management Framework), there is a growing emphasis on explainability and bias mitigation in AI security models.

The release of open-source multimodal models like OpenAI's CLIP and Meta's VideoMAE has accelerated progress in AI-based scene understanding.

Market and Industry Trends

Rising security concerns and the need for proactive threat mitigation have led to a surge in investments in AI-based security infrastructure at airports worldwide. The global airport security market is projected to grow significantly, driven by heightened security needs and regulatory compliance requirements.

Several governments and regulatory bodies have introduced new guidelines for AI-powered surveillance, emphasizing transparency, fairness, and data governance. Compliance with these regulations is becoming a critical requirement for AI-driven security solutions deployed in sensitive environments like airports.

# 3. Market access & Exploitation

## 3.1. Partners' market access

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

Each partner must update Market access of its' organisation on the ITEA Community website. There are two locations where a partner can update the Market access:

- ITEA Community website > Project page > Partners > Click relevant organisation in the list > Reporting > Click relevant PPR to update

or

- ITEA Community website > Project page > Partners > Click relevant organisation in the list > Partner details (click edit button on this page)

For more information, please check the latest version of the PPR instruction.

## 3.2. Top 8 cumulative project achievements

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

For more information about this section, please check the latest version of the PPR guideline.

## 3.3. Realised achievements

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

For more information about this section, please check the latest version of the PPR guideline.

# 4. Project progress during the reporting period

## 4.1. Project progress and issues during the reporting period

### 4.1.1. Top 4 technical achievements during the reporting period

*Identify and provide the 4 main technical achievements made during the reporting period. Do not simply list the deliverables as technical achievements. Focus on results that generate value (or enable value to be generated), i.e. outputs that bring you closer to your innovation and business goals.*

*This top 4 should provide the current technical highlights of the project that were achieved or completed during the reporting period.*

*For each identified technical achievement, provide some more details and - whenever relevant - clarifications on the actual nature of the achievement in approximately 50-70 words per achievement.*

*As a note: In the first semester(s) of the project, it is possible to have less than 4 technical achievements, in that case you can submit the available ones only.*

**1. AI-Driven Anomaly and Threat Detection Across Multi-Modal Inputs**

Several partners, including Alpata, ARD, Bosch, TU/e, and KoçSistem, advanced AI models capable of detecting anomalies, security threats, and criminal activities using multi-modal data (images, audio, vibrations, RF signals). Bosch developed a prototype AI model to fuse visible and thermal images for better detection in low-light conditions. TU/e implemented an AI-powered anomaly behaviour detection system, integrating privacy-preserving techniques for human monitoring. These developments significantly enhance security in critical environments like airports, ports, and construction sites.

**2. Scalable, AI-Driven SINTRA Airport Platform for Real-Time Data Processing**

TAV Technologies developed a robust platform based on Kafka, ClickHouse, HAProxy, and WebSockets, enabling real-time processing of sensor, radar, and camera data. The platform integrates advanced AI inference using NVIDIA DeepStream and TensorRT, ensuring high-speed anomaly detection and operational efficiency. It follows a zero-trust security model, incorporating federated learning, secure multi-tenancy, and GDPR compliance. This platform lays the foundation for smart airport security and operations, with future expansions planned for UAV integration.

**3. Automated AI Labelling System to Improve Model Training Efficiency**

TAV Technologies introduced "Auto Label Anything" (ALA), an automated data labelling tool leveraging Meta's Segment Anything Model (SAM). The tool supports multiple AI frameworks like TensorFlow and PyTorch, reducing the time and cost of manual data annotation. This innovation accelerates AI model training, improving the accuracy and efficiency of security and surveillance applications in SINTRA.

**4. Edge AI and Secure IoT Infrastructure for Real-Time Security Applications**

Sensolus, Sirris, and Inosens worked on edge AI, BLE-based tracking, and radar-based object detection for security and operational tracking. Sirris developed privacy-preserving image anonymization and fragile watermarking techniques, ensuring compliance with data protection regulations. Inosens made advancements in radar-based object detection using mmWave sensors, enabling AI-powered people tracking with enhanced 3D spatial awareness. These innovations support real-time security monitoring in diverse environments while addressing privacy, data integrity, and low-power IoT challenges.

*Copy the above template if more technical achievements need to be indicated.*

### 4.1.2. Top 4 next technical targets

*Identify and provide the 4 main technical targets planned for the forthcoming reporting period. Provide further details in approximately 50-70 words per target.*

**1. Advanced Anomaly Detection and AI Fusion Models**

The development and deployment of AI-powered anomaly detection systems will be enhanced, focusing on multi-modal AI fusion techniques. These models will integrate data from thermal cameras, IoT sensors, RF signals, and video feeds to improve anomaly detection accuracy, even in low-light conditions. AI-based detection models will be refined to identify security threats, criminal activities, and operational inefficiencies in airports, ports, and transportation hubs.

**2. IoT and Sensor-Based Data Processing Infrastructure**

The next phase will involve optimizing data retrieval from IoT sensors through API-based local server access. The focus will be on enhancing real-time data streaming, refining sensor integration methodologies, and improving data visualization for security and efficiency monitoring. Privacy-preserving techniques such as anonymization and encrypted data transmission will also be incorporated to comply with GDPR and cybersecurity regulations.

**3. AI-Powered Security and Surveillance Systems**

Continued advancements will be made in AI-powered surveillance, focusing on real-time security alerts, object tracking, and behavioural anomaly recognition. Technologies like YOLOv8-Pose and Zero-Shot Human Action Recognition will be further developed to reduce false alarms and improve

classification accuracy. These systems will be integrated into airport and transportation security infrastructures, ensuring rapid threat identification and automated incident response.

**4. Scalable, Secure, and Privacy-Enhanced Data Governance**

The project will enhance its security framework by strengthening role-based access control, implementing GDPR-compliant governance models, and integrating AI-driven threat detection mechanisms. Secure data-sharing solutions will be optimized for cross-platform communication, ensuring seamless integration among different infrastructure sectors, including airports, railways, and industrial sites. Blockchain and encryption-based security models will be explored for secure access and data integrity.

*Copy the above template if more next technical achievements need to be indicated.*

### 4.1.3. Top 4 issues

*This part should highlight the 4 main issues the project had to face during the reporting period. Issues can be related to: management, overall progress, technical bottlenecks, funding, a brand-new game-changing competitor, etc. Issues can typically be realised risks that were identified beforehand (they can also be related to unexpected events or results).*

*For each identified issue:*
*provide details in approximately 20-30 words per issue;*

- *indicate the impact on the project; and*

*explain which mitigation action has been (or will be) set up to solve the issue. Clarify if the current situation is the final one related to this issue or if there is still remaining impact to be dealt with, in approximately 20-30 words.*

*If needed, the project leader can identify up to 8 issues in the template reviewed by the STG. In this case, copy the necessary table rows and insert as new rows. However, it is important to properly select the 4 main ones, as only these will be visible in the final generated PPR.*

**1. Technical Bottlenecks in AI Model Training and Data Availability**

***Details***:

Several partners, including Bosch, ARD Group, and Inosens, faced difficulties in training AI models due to limited access to quality datasets. The lack of thermal image datasets required Bosch to develop a thermal image simulator, while Inosens had to conduct extensive data collection studies to ensure reliable AI model training for mmWave radar sensors. Additionally, ARD Group struggled with action recognition models due to inconsistencies in available open datasets, necessitating further pre-processing and adaptation efforts.

***Impact***:

Delays in AI model training reduce project efficiency, impacting predictive accuracy and real-world deployment. Additional data collection efforts increase costs and slow innovation.

***Mitigation action***:

Partnerships with relevant organizations (e.g., airports, smart city projects) to gain access to real-world datasets can be established. Synthetic data generation techniques, such as domain adaptation, GANs (Generative Adversarial Networks), or simulated environments to supplement real-world datasets (e.g., Bosch's thermal image simulator) can be used.

**2. Integration Challenges Across Different Platforms and Systems**

***Details***:

The integration of various AI models, sensors, and data sources posed significant challenges for multiple partners. TAV Technologies worked on ensuring seamless integration of high-speed camera streams, IoT sensors, and real-time AI inference within the SINTRA Airport Platform. However, aligning these components across different partners and infrastructure (e.g., Kafka, ClickHouse, HAProxy) required additional effort.

***Impact***:

Incompatibility between systems deteriorates real-time data processing and decision-making, causing inefficiencies in AI-driven automation and increasing project complexity and resource demands.

***Mitigation action***:

A standardized API framework, middleware solutions, and event-driven architectures (e.g., Kafka) can improve interoperability. Establishing cross-partner test environments will allow validation before deployment. Edge AI solutions and improved data format alignment can help integrate drone-based and ground-based AI models more effectively, reducing system fragmentation and ensuring real-time processing.

**3. Data Security, Privacy, and Regulatory Compliance**

***Details***:

Data governance and compliance with GDPR and other security regulations were major concerns, particularly for partners handling sensitive video and sensor data. SafeCity developed a cybersecurity assessment framework, but the rapid deployment of IoT and AI technologies introduced new risks that required ongoing mitigation strategies. Sirris and TU/e worked on privacy-preserving AI models, yet ensuring compliance while maintaining detection accuracy remained a complex challenge.

***Impact***:

Non-compliance risks legal penalties and reputational damage. Privacy issues may reduce stakeholder trust, while security vulnerabilities expose systems to cyber threats.

***Mitigation action***:

Privacy-preserving AI techniques, such as homomorphic encryption, differential privacy, and advanced anonymization methods can be refined. Role-based access controls, zero-trust security, and continuous audits will strengthen data governance. Developing incident response plans and AI ethics guidelines can proactively address cybersecurity risks associated with rapid IoT and AI deployments.

**4. Delays in Hardware and Sensor Deployments**

***Details***:

Hardware procurement and sensor deployment delays affected various work packages. Avular experienced delays in assembling the Vertex Drone due to supply chain issues, impacting the timeline for field tests. Similarly, MantiSpectra faced issues with sensor stability, requiring additional internal tests and adjustments to improve signal-to-noise ratios before deployment.

***Impact***:

Postponed deployments disrupt testing schedules, delay AI model validation, and impact project milestones, leading to cost overruns and potential missed business opportunities.

***Mitigation action***:

Alternative suppliers and establish backup procurement plans to mitigate the impact of supply chain disruptions (e.g., Avular's Vertex Drone delays) can be identified. Parallelizing software and hardware development ensures progress despite delays. Interim prototyping with available hardware allows testing before final deployment. Rigorous in-lab stability testing, phased deployment strategies, and flexible integration plans can prevent delays from impacting project timelines.

*Copy the above template if more issues need to be indicated.*

### 4.1.4. Status of deliverables

*Indicate the status of the deliverables. If available, include the Gantt chart or any other overview that shows the progress of project tasks and the status of deliverables.*

**[Planned] What is the total number of deliverables in the project?**

The total number of deliverables in the project is 30.

**[Planned] How many deliverables are supposed to be finalised (from the start of the project until the end of this reporting period)?**

From the start of the project until the end of this reporting period, 13 deliverables are supposed to be finalised. These are:

- D1.1 Use case analysis and stakeholder requirements,
- D1.2 Hardware architecture and communication specifications,
- D1.3 Sensor and data source inventory report,
- D1.4 Privacy and data governance analysis report,
- D1.5 Use case specific sensor and data source integrations,
- D1.6 Platform architecture design document,
- D4.1 Data governance protocol,
- D4.2 Data management plan,
- D5.1 Public/internal website,
- D5.2 Dissemination and communication plan,
- D5.3 State-of-the-Art analysis,
- D6.1 Project and risk management plan,
- D6.2 Progress and quality assurance report 1 (M12).

**[Actual] How many deliverables have already been finalised (from the start of the project until the end of this reporting period)?**

From the start of the project until the end of this reporting period, 13 deliverables have already been finalised. These are:

- D1.1 Use case analysis and stakeholder requirements,
- D1.2 Hardware architecture and communication specifications,
- D1.3 Sensor and data source inventory report,
- D1.4 Privacy and data governance analysis report,
- D1.5 Use case specific sensor and data source integrations,
- D1.6 Platform architecture design document,

- D4.1 Data governance protocol,
- D4.2 Data management plan,
- D5.1 Public/internal website,
- D5.2 Dissemination and communication plan,
- D5.3 State-of-the-Art analysis,
- D6.1 Project and risk management plan,
- D6.2 Progress and quality assurance report 1 (M12).

**[Delayed] Are there any deliverables delayed more than 2 months in this reporting period? If so, please explain why.**

No, there are not any deliverables delayed.

*If useful, include the Gantt chart that shows the progress of project task and status of deliverables.*

### 4.1.5. Statement on project progress during the reporting period

*Explain the current global status and progress of the overall project in approximately 100 words. Indicate any possible change or delay that occurred during the reporting period, as well as its cause.*

*Do not report detailed technical progress of each WP here. The progress per WP can be reported in Chapter 4.2 of this PPR. Do not report on achievements from previous reporting periods (if such past achievements are required to better understand the current achievements, then state clearly that they are from previous reporting periods).*

*The level of the international collaboration might be mentioned here whenever relevant.*

The SINTRA project is advancing AI-driven security and anomaly detection across airports, ports, and construction sites. WP1 has focused on defining use cases, system architecture, and integrating key technologies such as cameras, IoT sensors, and AI models. WP2 has progressed in data collection, governance, and sensor integration. WP3 has developed multi-modal AI models for image, sound, and radar-based anomaly detection. WP4-6 emphasize platform architecture, industry collaborations, and dissemination efforts. Key achievements include AI-powered surveillance, privacy-preserving techniques, and real-time threat detection. Consortium partners continue refining security

frameworks, ensuring GDPR compliance, and improving AI model accuracy for real-world deployments.

## 4.2. Details of progress per Work Package

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

Each WP leader must provide input on the following location: ITEA Community website > Project page > Management > Reporting > Select the current PPR to report >Work Package progress.

For more details, check the latest version of the PPR instruction.

## 4.3. Per partner progress during the reporting period

*This instruction is for Chapters 4.3.1 and 4.3.2 of this PPR. These chapters are auto-generated. All project partners need to fill in all the required fields in their respective "Reporting" tab on the ITEA Community website.*

### 4.3.1. Partners' main contribution and effort

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

All project partners must provide input on the following location: ITEA Community website > Project page > Partners > Click Relevant organisation in the list > Reporting > Click relevant PPR to update.

Project coordinators must initiate the PPR for the current reporting period on the website, so that the rest of partners can access the current PPR reporting section. For more information please check the latest version of the PPR instruction.

### 4.3.2. Actual vs. planned effort overview

**Auto-generated section**: Do not edit or remove this box and do not provide any text in this chapter but provide the requested information directly on the ITEA Community website.

All project partners must provide input on the following location: ITEA Community website > Project page > Partners > Click Relevant organisation in the list > Reporting > Click relevant PPR to update.

Project coordinators must initiate the PPR for the current reporting period on the website, so that the rest of partners can access the current PPR reporting section. For more information, please check the latest version of the PPR instruction.

## 5. Additional feedback to previous STG remarks (optional)

*This chapter is meant to provide additional information on the status of previously defined actions by the reviewers (in addition to the information in the comment-field of the Project action list tool on the ITEA website). Use this chapter to provide more detailed information on how the reviewers can verify the updated action status. The status of the actions must be updated in the online project action list (under Management>Project Action list).*

*The aim of the Project action list tool is to react on the previous remarks from the Steering Group (STG), i.e. from the latest FPP evaluation, CR evaluation, latest PPR and/ or review. It can also be used to ask for recommendations from the STG (in which case the question should be detailed enough for any feedback to be possible).*

**To STG reviewers**: This chapter is meant to provide additional information on the status of actions, in addition to the information on the online action tool (the information is exported on the Excel file). The project consortium uses this chapter to provide longer and more detailed information that are too exhaustive for online action tool and the Excel export.

< >