# 2026-H1 Project Progress report

## SINTRA

Edited by: All Partners

Date: 28.09.2026

# Project key data

## ACRONYM and full-length title

| 22006 | SINTRA |
|---|---|
| Program Call | ITEA Call 2022 |
| Full-length Title | Security of Critical Infrastructure by Multi-Modal Dynamic Sensing and AI |
| Roadmap Challenge | Safety and Security |

## Project duration and size

| Size | Effort: 184.2 PY | Costs: 18.6 M€ |
|---|---|---|
| Time frame | Start: 01-12-2023 | End: 30-11-2026 (36 months) |

## Coordinator

| TAV Technologies | TAV Technologies |
|---|---|
| Type | Large Industry |
| Contact Person | Mr. Selim Sarı |
| Email Address | selim.sari@tav.aero |

## Project Status

| Latest FPP | Change Request (15-09-2026) |
|---|---|
| Latest PPR | 2025 Semester 2 |
| Latest Review | SINTRA #2 (a.m.) (29-01-2026) |
| Upcoming Review | SINTRA final (a.m.) (20-11-2026) |
| PCA status | SINTRA PCA.pdf (Signed: 28-01-2026) |

## Consortium

| Country | Funding Status | National Coordinator (Company) | Total Effort (PY) | List of Partners |
|---|---|---|---|---|
| Belgium | Funded (Y) | Farhad Aghili (SIRRIS) | 28 PY | Airobot, C-SITE, Citymesh, Macq, Sensolus, SIRRIS, SkyeBase |
| Finland | Funded (Y) | Markus Sihvonen (University of Jyväskylä) | 59 PY | 2NS Cybersecurity Oy, Abloy Oy, Hoxhunt Oy, Jyväskylän ammattikorkeakoulu, Port authority, Secapp Oy, Sensoan Oy, Teleste, University of Jyväskylä |
| The Netherlands | Funded (Y) | Egor Bondarev (Eindhoven University of Technology) | 57 PY | Avular Innovations B.V., Eindhoven University of Technology, IQSight, MantiSpectra, Omines Internetbureau B.V., Port of Moerdijk, SafeCity B.V., Sorama B.V., ViNotion BV |
| Türkiye | Funded (Y) | Selim Sarı (TAV Technologies) | 41 PY | ARD GROUP, inosens, KoçSistem, Koçtaş Yapı Marketleri Tic. A.ş, Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş., TAV Technologies |

## Project Acronyms

| | |
|---|---|
| AI | Artificial Intelligence |
| API | Application Programming Interface |
| AIS | Automatic Identification System |
| ANPR | Automatic Number Plate Recognition |
| BLE | Bluetooth Low Energy |
| CCTV | Closed-Circuit Television |
| CER | Critical Entities Resilience |
| DECT NR+ | Digital Enhanced Cordless Telecommunications – New Radio Plus |
| IOT | Internet of Things |
| IP67 | Ingress Protection Rating 67 |
| IR | Infrared |
| KPI | Key Performance Indicator |
| LiDAR | Light Detection and Ranging |
| LTE-M | Long-Term Evolution for Machines |
| MQTT | Message Queuing Telemetry Transport |
| NATO | North Atlantic Treaty Organization |
| NB-IoT | Narrowband Internet of Things |
| NIS2 | Network and Information Systems Directive 2 |
| OPC UA | Open Platform Communications Unified Architecture |
| OT | Operational Technology |
| PIR | Passive Infrared |
| RGB | Red, Green, Blue |
| UAV | Unmanned Aerial Vehicle |
| VAR | Unmanned Aerial Vehicle |

# Table of contents

Project key data ..... 2
ACRONYM and full-length title ..... 2
Project duration and size ..... 2
Coordinator ..... 2
Project Status ..... 2
Consortium ..... 2
Project Acronyms ..... 3
Table of contents ..... 4
1. Project one-page description ..... 5
2. Project overall status ..... 6
2.1. Top 4 overall targeted innovations ..... 6
2.2. Top 4 overall targeted business impacts ..... 7
2.3. Top 4 overall project KPIs ..... 9
2.4. Top 4 overall risks ..... 10
2.5. Change in the technology and market during the reporting period ..... 11
3. Market access & Exploitation ..... 13
3.1. Partners' market access ..... 13
3.2. Top 8 cumulative project achievements ..... 19
3.3. Realised achievements ..... 21
4. Project progress during the reporting period ..... 22
4.1. Project progress and issues during the reporting period ..... 22
4.2. Details of progress per Work Package ..... 28
4.3. Per partner progress during the reporting period ..... 33
5. Additional feedback to previous STG remarks (optional) ..... 40

# 1. Project one-page description

Stakeholders of critical industrial and civil infrastructures, such as airports, harbours, construction sites and other large-scale public environments, are exposed to a wide range of safety and security threats. These threats range from organised criminal activities to vandalism, theft, violence, intrusion and other disruptive events. Although modern surveillance and security platforms increasingly incorporate video analytics and centralized monitoring, operational decisions are still frequently based on fragmented information from isolated systems and organisational silos.

Existing solutions often rely heavily on video data and have limited capability to correlate heterogeneous information across sensors, systems and organisations. This restricts the detection and interpretation of complex, context-dependent threats and reduces the ability of operators to build a common situational picture. In addition, interoperability, data governance, privacy protection and secure information exchange remain important challenges when security information needs to be shared across public and private stakeholders.

SINTRA addresses these limitations through an open, AI-enabled data-streaming and analytics platform designed to support trustworthy cross-organisational safety and security monitoring. The platform facilitates secure information exchange, multimodal data integration and coordinated analysis across participating stakeholders, while taking privacy, data governance and ethical requirements into account. This enables security operators to move from isolated monitoring towards broader situational awareness and more informed operational decision-making.

From a technology perspective, SINTRA advances beyond conventional surveillance by combining heterogeneous sensing modalities and AI-based analysis. Visual, acoustic, radar, multispectral, LiDAR, passive infrared and environmental sensor data can be integrated with existing operational data sources to provide a richer representation of the monitored environment. Current project developments include intelligent CCTV infrastructures with real-world localization, modular perimeter sensing, multimodal anomaly detection, pedestrian intent prediction, and integrated detection, localization and follow-up capabilities. In the airport use case, conventional CCTV infrastructure is enhanced through multimodal event detection and LiDAR-assisted camera-to-world mapping, enabling physical localization of detected events and improved situational awareness.

# 2. Project overall status

## 2.1. Top 4 overall targeted innovations

**1. Smartized CCTV Infrastructure for Real-Time Multimodal Airport Incident Detection and Localization**

***Main contributors***: TAV Technologies, ARD Group, INOSENS, ALPATA

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

Current airport CCTV systems mainly provide video monitoring, while incident localization and cross-camera event correlation still require significant manual effort. SINTRA introduces a smartized CCTV infrastructure that transforms conventional cameras into intelligent sensing assets by combining real-time object detection, anonymous multi-object tracking, multimodal event correlation, and camera-to-world coordinate mapping. Using LiDAR-assisted calibration, camera observations can be linked to physical locations, enabling automatic identification of relevant cameras and improved incident understanding. The solution further combines CCTV analytics with sensor-based anomaly detection and AI-based event interpretation to provide explainable operational decision support for airport security and safety operations.

**2. Smart realtime advanced modular analytics platform**

***Main contributors***: Sensoan Oy, Abloy Oy, Port of Kemi, University of Jyväskylä

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

**Modular platform.** The containerized SINTRA platform supports local or remote analysis, accommodating sensitive data and transfer and computing requirements. Kemi's installed surveillance system supplies data enriched by embedded edge AI and context metadata, retaining only relevant video feeds. Context-Driven Multimodal Fusion supports creation of a situational picture, with broader situational-awareness and decision support planned. The northern seaport setting provides demanding conditions for developing anomaly detection, particularly from visual and audio data.

**Field KPIs.** The sampled export covering 6–11 September 2026 represents about 4.4 days of routine operation. Median transport latency increases from 7 ms at one hop to 82 seconds at five hops; the maximum observed was 141 seconds. Two of six nodes generate 92% of passive infrared (PIR) events, with spatial factors appearing more influential than daylight in this dataset. False-alarm reduction is not yet established. Missing ground-truth labels prevent measurement of missed-threat rates and precision/recall, while missing operator and resolution timestamps limit incident-response KPIs. Audio and rare-event KPIs remain unassessed, and privacy risks from linking streams to external systems remain under review.

**Architecture and remaining development.** Prototype nodes combine modular radios, a custom baseplate and commercial IP67 enclosures. Fence deployments behave mainly as chains, with test-

fence communication demonstrated up to 90 metres. A separate DECT NR+ NATO exercise demonstrated a star network with autonomous sensing and unmanned-vessel data collection over an apparently multi-kilometre range. Remote firmware updates and the live API feed to the University of Jyväskylä are operational. Priorities include sensor fusion, true self-routing mesh operation and enclosure reliability, following suspected moisture-related reboots in one Kemi node.

**3. AI-Based Pedestrian Crossing Intent Prediction for Proactive Safety Monitoring**

***Main contributors***: Macq, Sirris

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

Conventional video analytics mainly detect and track pedestrians based on their current position, providing limited information about their likely next actions. SINTRA advances this towards proactive safety monitoring by predicting pedestrian crossing intent from camera feeds. The solution combines pedestrian detection, robust tracking and re-identification, pose information, motion history, geometrical road-side definitions and camera-to-real-world coordinate mapping with an XGBoost-based intent classifier. It distinguishes pedestrians expected to cross within a defined prediction horizon from those not crossing, with the best results currently obtained for predicting crossing up to three seconds ahead.

**4. Full-cycle 24/7 Criminals' Multimodal Monitoring: Detection, Re-identification, Follow**

***Main contributors***: TU/e, Vinotion, Avular, Omines, SafeCity, IQSight, INOSENS, Port of Moerdijk

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

At present, there are neither academic, nor industrial literature reports on full-cycle 24/7 criminal's monitoring at critical infrastructure premises. Existing solutions either propose a single multi-modal sensor suite for crime detection that works statically (in isolation) or propose re-identification functionality across multiple static cameras (no drones), or provide the follow-me functionality for a UAV surveillance.

At the final year of SINTRA, we have developed and integrated the all-in-one pipeline with a visualization dashboard for control room operators that combines all required functionality for automated detection and capture of suspects: a) multi-modal sensor suites (both on static poles and on drones) that perform 24/7 monitoring in four modalities together (visual, IR, acoustic and radar), b) aggregate all the detected suspect data into a dashboard run at the control officers centre, c) performs search and re-identification of suspects in the data coming from all sensors located at the premises, d) launches UAVs (with RGB and IR sensors) to find the suspects by the re-identification algorithms and c) follow the detected suspect by the drone that has re-identified the suspect.

## 2.2. Top 4 overall targeted business impacts

**1. Operational Intelligence and Automated Incident Response for Airport Security Operations**

***Short description***: The innovation transforms conventional CCTV infrastructures into intelligent operational systems capable of automatically detecting, localizing and correlating security-related events.

By combining video analytics, multi-object tracking, multimodal AI and sensor-triggered verification, the solution reduces manual monitoring effort, accelerates incident response and improves situational awareness. The approach enables airport operators to manage large-scale surveillance networks more efficiently while providing explainable evidence and decision support for security and operational teams.

***Main contributors***: TAV Technologies, ARD Group, INOSENS, ALPATA

***Market / competitors***:

The primary target market includes airports, airport operators, airport technology providers and critical infrastructure operators seeking to enhance existing CCTV systems with AI-driven situational awareness and automated incident management capabilities. The solution addresses operational safety, security monitoring and surveillance optimization use cases in large-scale environments. Key competitors include SITA, Amadeus Airport IT, Thales, Collins Aerospace, Dormakaba Airport Solutions, Genetec, and Advancis.

**2. A local sensor node and a multi-radio extended-range sink**

***Short description***: We have developed two new prototype product lines; both originally aimed at perimeter monitoring but not limited to it. The first is a sensor node built for BLE/Wirepas mesh networks. We already have a working design and a sample unit. The second is a companion device that extends the network's range using DECT NR+, LTE-M, or NB-IoT. It doesn't need the first product to work; it can run on its own, for example listening directly to BLE beacons. Both are still being developed and tested.

***Main contributors***: Sensoan

***Market / competitors***:

Edge data collection, OPC UA/MQTT, real-time streaming, processing, anomaly detection and dashboards. Azure IoT Operations provides an industrial edge data plane and can process/normalize OT data before cloud analytics.

We're already seeing interest from potential clients across several critical infrastructure sectors. Part of that is because these products aren't tied to perimeter monitoring specifically. They can be applied to other use cases too, and that's widened the interest even further. That tells us the opportunity here is bigger than one application, and we're actively looking at where else this technology could go.

Pairing a low-power mesh sensor with a flexible, independently operable long-range device gives us room to cover very different deployment needs. Small battery-powered setups on one end, longer-range configurations for bigger sites on the other. We think that flexibility is a real advantage when talking to different types of infrastructure operators.

**3. AI-Based Pedestrian Crossing Intent Prediction for Proactive Safety Monitoring**

***Short description***: We use RGB camera images to monitor Vulnerable Road Users. Using the history of their pose we predict a few seconds ahead their intention.

***Main contributors***: Sirris, Macq

***Market / competitors***:

There has already been a lot of research in the detection of pedestrians. Also, in automated cars. We see this as an upselling possibility to enhance the capabilities of cameras that serve other purposes like ANPR. Competitors are Tattile, Milesight and Hikvision.

**4. Full-cycle 24/7 Criminals' Multimodal Monitoring: Detection, Re-identification, Follow**

***Short description***: See the description of the system in the previous section. Currently, a lot of potential customers show interest in this part of the SINTRA solution: Port of Moerdijk already asked us to keep the system after the project. National Dutch police are coming to see the demonstrator in October 2025. Port of Rotterdam officers are engaged with their interest. North Sea Port is also engaged.

***Main contributors***: Vinotion, TU/e, Avular, Sorama, INOSENS, Omines, SafeCity, IQSight

***Market / competitors***:

BriefCam, Genetec

## 2.3. Top 4 overall project KPIs

| | Initial value | Targeted value | Current value |
|---|---|---|---|
| **1. LiDAR-Assisted CCTV Localization Accuracy** | N/A | 90% | 90% |

This KPI measures the system's ability to estimate person positions within the monitored area within a predefined spatial tolerance.

| | | | |
|---|---|---|---|
| **2. Sensor Event Distribution / Coverage** | N/A | 90% | 92% of PIR events generated by 2 of 6 nodes |

This KPI measures how sensor-triggered events are distributed across the deployed PIR nodes, providing an indication of spatial coverage and identifying whether event detection is concentrated in specific sensor locations.

| | | | |
|---|---|---|---|
| **3. Reduction of time to detect an incident** | N/A | Improve SotA (4-sec before the move) by 10% | 5-sec before the move |

Time elapsed between the occurrence of an incident and its detection by the system.

| | | | |
|---|---|---|---|
| **4. Reduction of false alarm rate for anomaly detection (at Port of Moerdijk)** | 25% | 4% | 8% |

Percentage of anomaly detection alerts that are incorrectly triggered under normal, non-anomalous conditions.

## 2.4. Top 4 overall risks

| | Severity | Probability | Stage |
|---|---|---|---|
| **1.** Lidar Based Localization Performance | Medium | Possible | Monitoring & Controlling |

***Avoidance action***:

To prevent performance degradation in multi-camera tracking and incident localization, continuous validation activities are being conducted using representative CCTV datasets and manually verified ground truth annotations. Camera calibration procedures, tracking consistency checks, and localization accuracy assessments are integrated into the development lifecycle. Regular benchmarking against project KPIs is performed to ensure that detection, tracking, and localization components achieve the required performance levels.

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

If tracking and localization performance remains below target values, component-level optimisation will be prioritised, and confidence-based validation mechanisms will be introduced.

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

Algorithm development, system integration, and validation activities during the current and forthcoming reporting periods.

| | | | |
|---|---|---|---|
| **2.** Unproven detection accuracy | Medium | Possible | Monitoring & Controlling |

***Avoidance action***:Assign one accountable owner and a measurable closure criterion to each risk. Review the unresolved technical and validation risks weekly, with a formal reassessment before operational acceptance.

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

Run controlled, labelled intrusion and normal-operation tests across locations, weather and lighting conditions. Agree acceptance thresholds; record event, alert, acknowledgement and resolution timestamps. Investigate sensor placement before changing daylight settings.

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

Until the end of the project.

| | | | |
|---|---|---|---|
| **3.** Pedestrian Crossing Intent Prediction Performance | Medium | Possible | Mitigating |

***Avoidance action***:

To reduce incorrect pedestrian intent predictions, the detection, tracking and classification pipeline is being continuously refined and validated. Improvements include robust pedestrian re-identification after occlusions, filtering of false pedestrian detections, stricter pose-point validation, real-world coordinate mapping, and optimisation of the XGBoost-based intent classifier for different prediction horizons.

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

If the required classification performance cannot be achieved for all intent classes, particularly the challenging **"Waiting"** class, the system will prioritise the more reliably classified **"Crossing"** and **"Not Crossing"** cases and further optimise the classification pipeline based on representative data and deployment conditions.

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

Algorithm optimisation, deployment on the Macq camera, system integration and final validation activities until the end of the project.

| | | | |
|---|---|---|---|
| **4.** Regulatory constraints on deployment of UAVs at premises | Critical | Almost certain | Monitoring & Controlling |

***Avoidance action***:

Start filing the request for UAV flights in the area with authorities a year in advance. With respect to the autonomous flight clearance, press authorities to make exceptions for this case. Motivate the exception by high impact of possible disruptions in the premises of the critical infrastructure.

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

No feasible back-up plan possible. This is a must for high-end full-area surveillance. Mitigation can be done by installing thousands of static cameras at every corner of the premises. However, this incurs very high costs.

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

From now on and after the project, when the system is in deployment at premises.

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

Since the last reporting period, the external technological landscape has continued to evolve towards the operational deployment of AI-enabled security systems and intelligent surveillance infrastructures. Across airports, ports and other critical infrastructures, organizations are increasingly prioritizing production-ready solutions that combine AI analytics, cybersecurity, operational resilience and measurable return on investment rather than standalone experimental AI deployments. This broader shift is also reflected in Genetec's *2026 State of Physical Security Report*, which highlights a significant increase in interest in AI adoption and shows that more than 70% of surveyed organizations are already using unified or integrated physical security systems. The report further indicates that physical security

is increasingly evolving beyond its traditional protective role into a strategic function that supports operational awareness, cross-functional collaboration and business decision-making (Genetec, 2025).

Regulatory developments continue to shape the market. The implementation of the EU AI Act has increased the importance of transparency, traceability, human oversight and governance requirements for AI-enabled systems. This is particularly relevant for AI systems used as safety components in critical infrastructure, which may be classified as high-risk under the Act depending on their intended function and potential impact. As the regulatory framework is progressively implemented, explainability, auditability and compliance-by-design are therefore becoming increasingly important design considerations for AI solutions deployed in European critical infrastructure environments (European Commission, 2026; EU Artificial Intelligence Act, 2026).

At the same time, cybersecurity and resilience requirements have become increasingly prominent with the ongoing implementation of the NIS2 Directive and the Critical Entities Resilience (CER) framework. NIS2 strengthens cybersecurity requirements across highly critical sectors, including air transport and digital infrastructure, with particular emphasis on cybersecurity risk management, incident reporting, supply-chain security and business continuity. In parallel, the CER Directive establishes a broader resilience framework requiring critical entities to strengthen their ability to prevent, withstand, respond to and recover from disruptive incidents. These developments are increasing the importance of cyber-physical resilience considerations in the design and deployment of security systems (ENISA, 2026; European Union, 2022).

Overall, the technological and business relevance of AI-driven multimodal security systems remains strong. Compared with previous reporting periods, market differentiation is increasingly influenced by regulatory readiness, cybersecurity and resilience, operational integration, deployment scalability and the ability to transform existing surveillance infrastructures into broader situational-awareness and decision-support platforms, rather than by standalone AI model performance alone.

# 3. Market access & Exploitation

## 3.1. Partners' market access

| | | | |
|---|---|---|---|
| Hoxhunt Oy | sme | FIN | 16 PY |
| Hoxhunt's customer base has grown 50% over the last year, allowing directly selling new innovations throuhg the SaaS model to wider audience. Hoxhunt works with large enterprise customers across the globe including key critical infrastructure companies. Hoxhunt has actively expanded target markets in Europe, US and Asia. | | | |
| TAV Technologies | ind | TUR | 14 PY |
| Up to the current reporting period, TAV Technologies has focused on transforming SINTRA's technical developments into exploitable airport solutions by validating AI-based video analytics, event-driven incident detection, multimodal data fusion, and camera–LiDAR calibration approaches in representative operational environments. These activities have strengthened the integration potential of SINTRA with existing airport surveillance, AOCC and maintenance ecosystems, while demonstrating how legacy CCTV infrastructure can be enhanced without major hardware replacement. Technical validation has also supported the definition of scalable deployment scenarios for security, operational monitoring and predictive maintenance use cases.<br><br>In the next period, exploitation activities will focus on final pilot validation, performance benchmarking, integration maturity and commercialization readiness. TAV Technologies will further assess deployment models for airports within its existing customer network, including potential opportunities in Europe and LATAM. Future steps will also include refining the value proposition, identifying integration. | | | |
| University of Jyväskylä | uni | FIN | 14 PY |
| For us, the industrial challenges and co-operation fuel further innovations. Companies and universities jointly develop new knowledge and innovations as per business demand. The joint effort accelerates the use of research knowledge, strengthens networks in situational awareness, privacy and security, and digital sovereignty. Co-innovation enables fast feedback loop to early integration, which would not be available without it. University of Jyväskylä uses new knowledge and competence gained in the project to create new directions for research and IPR, in technology transfer to companies, especially in situational awareness, privacy and security. The project enables creation of tailored research results for critical needs of companies and their business. The project will create proofs-of-concepts, aiming at validation of novel solutios. High-quality publications and experimental research work make the co-innovation together with companies more effective.<br>In the project, we strenghten early detection and prevention of threats, threat analysis, vulnerability management, incident response, and resilience | | | |
| Eindhoven University of Technology | uni | NLD | 9 PY |
| TU/e is an education institute and does not sell products, but supports industrial partners with innovations and algorithms on AI sensor data processing and fusion. In more detail, TU/e will provide an advanced algorithms for image analysis, detection of behaviour anomalies, and smart sensor network to the project partners to be further integrated into their products. These algorithms will be packaged as components and shipped to the industrial partner (e.g. ViNotion, Avular) for integration. Besides this, TU/e uses the research results obtained in the project to enhance the master program course 5LSH0 "Computer vision and 3D data processing". | | | |
| IQSight | ind | NLD | 10 PY |
| IQSIGHT is well positioned to exploit the results of the SINTRA project through its established global network of distributors and system integrators, providing strong access to the critical infrastructure surveillance market. The company already has a significant presence in the Netherlands, serving as a technology partner in major deployments such as Amsterdam Schiphol Airport and Eindhoven city center. Building on its expertise in advanced IP camera platforms, IQSIGHT aims to commercialize innovative imaging solutions that improve the robustness and reliability of AI-based surveillance systems. The SINTRA platform's integration of multi-sensing technologies will enable IQSIGHT to offer fully integrated solutions rather than standalone hardware products, creating a clear competitive advantage. This strengthens the | | | |

| | | | |
|---|---|---|---|
| company's leadership in the intelligent video surveillance market, expand its share of the growing thermal network camera segment, and target an additional 2% of global critical infrastructure protection revenue over the five years following project completion. | | | |
| ViNotion BV | ind | NLD | 9 PY |
| On June 1st, Nedinsco was acquired by Hensoldt, a world-leading player in the field of optronics systems. This opens new market access on a world scale. Hensoldt is very much interested in the Sintra development by ViNotion. In the coming period we will investigate how to leverage the exploitation of results via Hensoldt. | | | |
| 2NS Cybersecurity Oy | sme | FIN | 8 PY |
| During this reporting period, 2NS further explored the commercial potential of AI security and threat analysis services, particularly in relation to AI-related attack vectors and enhanced security monitoring. The knowledge gained within the project is being used to refine potential service concepts and future market offerings. In the next period, 2NS will continue assessing how these capabilities can be integrated into its cybersecurity services and commercialized for relevant customer segments. | | | |
| Koçtaş Yapı Marketleri Tic. A.ş | ind | TUR | 8 PY |
| Koctas as a retailer has more than 335 physical stores both fix and big concepts. After the SINTRA's solution will be delivered to the market, Koctas aims to expand it to all its stores in Turkey. Moreover, the solution as a platform will be planned to be sold to retailers in Turkey and to neighbor countries. Parallel to the domestic process, Koctas will spread the solution to Europe by the help of its partner Kingfisher PLC from UK which operates with its brands in 8 countries. | | | |
| Avular Innovations B.V. | sme | NLD | 7 PY |
| Commercial impact for Avular through the participation in the Sintra project is foreseen on two levels:<br>-direct commercialization: sales of mobile robots and related equipment fit for the purpose of safety and security monitoring. Clients could include the Dutch end-user or similar market players. In addition, it is possible that Avular technologies will be sold to end-users of other use cases in the Sintra project. Outside the project Avular has standing relationships with a variety of infrastructural asset owners that are interested in the solutions developed in the project. For example, in 2024 Dutch Railways infrastructure owner ProRail has shown interested in our UGV for safety inspection of Rail Yards and we've conducted the first feasibility tests.<br>xisting markets. | | | |
| MantiSpectra | sme | NLD | 7 PY |
| MantiSpectra is commercialising unique near-infrared (NIR) sensors that can classify and quantify material composition using NIR light. Our ChipSense™ technology is the smallest and cheapest NIR sensor on the market, with a footprint of only ~4 mm squared, ultra-low power consumption, and suitability for volume production.<br>This tiny sensor can be integrated directly into the production line to monitor and control processes, increasing efficiency; across the production and logistics chain for quality control and product authenticity; and at the point of care for effective health monitoring. The technology also has potential applications in the forensic sector for real-time, on-site identification of drugs and explosive materials.<br>• The TRL level of the sensor module will be increased following the on-field validation studies with end users in this t.<br>• We expect that the innovations from this project will be relevant and lead us to various new technical capabilities within our reach. | | | |
| ARD GROUP | ind | TUR | 6 PY |
| Security solutions became one of the leading operation fields of ARD GROUP. It established Dallmeier Turkey Electronic Inc. in 2022 providing high-end AI video imaging and analytics, tailored for the stringent requirements of various domains.<br><br>ARD GROUP has provided IT Infrastructure modernization solutions for the Ministry of Defense as well as video analytics solutions for the Istanbul Municipality and logistics management solutions for Disaster and Emergency Management Presidency in Türkiye. It has been providing tailored security solutions for governmental organizations. Today, ARD has reached over 30 million daily transactions from 500.000+ users. | | | |

| | | | |
|---|---|---|---|
| ARD aims to transform its know-how and provide R&D contribution to SINTRA which will result in a commercialized, secure, usable and expandable solution for its network. | | | |
| inosens | sme | TUR | 6 PY |
| INOSENS will install demo systems in TAV facilities. INO intends to pursue business opportunities in AI enabled sensing and AR solutions in Turkey and in Europe. INOSENS promotes dissemination materials well as participating in industry events to promote the new developed product.<br><br>Realizing the vision of "AI-based sensing technologies" outlined in its initial proposal, INOSENS has successfully developed the mmWave Radar Crowd Analytics System and proven its industrial validity through real-world data collected at İAM Airport.<br>Through these implemented strategies, the SINTRA project is now ready for commercialization as a high-accuracy human tracking system that is fully compliant with privacy regulations, cost-effective, and operationally robust.<br><br>As INOSENS, we have also defined product branding which is AuraSens-r for the output of this project. | | | |
| Jyväskylän ammattikorkeakoulu | uni | FIN | 6 PY |
| One of Jyväskylä University of Applied Sciences' (Jamk) basic missions is R&D work that serves the business community in its region. Jamk has been as forerunner in developing Finland's national resilience already 15 years. In practice, this takes the form of cybersecurity-related R&D work in cooperation with companies in various sectors. Our partners include SMEs, large companies and public actors, as in this project. In addition to RDI, we provide cybersecurity and data analytics training, testing and development services using the advanced Realistic Global Cyber Environment (RGCE) and its computing cluster, which are isolated from public networks. These development environments enable applied research, experimentation, testing and demonstration based on the individual needs of companies, which are characteristic of JAMK's RDI activities. With its know-how and advanced technological environment, Jamk is in a strong position to support the development and commercialisation of products and services for companies. | | | |
| Macq | sme | BEL | 6 PY |
| Macq's customers are municipalities, local and federal police zones, traffic centers and road operators. The market operates by tenders unless there is a unique product offering. Our sales model allows both selling of products installed by integrators and as-a-service solutions.<br><br>We have created sales material to help our partners. To help them create quotations for the tenders a shop has been set up.<br>We destinguish two different kind of critical infrastructure: large area and points. The first are harbours and airports. An example of the second are railway crossings.<br><br>In Flanders there are 314 ‘black’ dangerous road crossings. In the Netherlands 1.900. In France 15.405. There are a lot of market opportunities for new innovative traffic and mobility solutions to monitor the infrastructure but also protect the traffic participants.<br><br>Exploring markets in India, Africa and South-America giving the first commercial successes using the as-a-service approach Drive For Zero (https://driveforzero.eu/nl_BE) | | | |
| Omines Internetbureau B.V. | sme | NLD | 6 PY |
| Since 2014 Omines has participated in many cutting edge innovative Smart City projects, positioning itself as a specialist in real-time actionable data processing, combining AI vision-based and IoT sensor data with automated responses. Our software has been integrated in varying applications in the public space, from automated security monitoring to logistic systems. As our software cannot be isolated or used separately from its data influx, we support our project partners to enhance their products through UI/UX, automation of processing and the conversion of data in actionable information, events and reports.<br><br>We intend to further solidify ourselves, primarily in the Netherlands but also in Western Europe as a whole, as a specialist in Smart Data processing systems, providing affordable and workable solutions in these markets to innovative parties that either cannot (yet) realize their ambitions using off-the-shelf products or need specific custom integrations or extensions. | | | |

| | | | |
|---|---|---|---|
| Sorama B.V. | sme | NLD | 7 PY |
| During this reporting period, Sorama further evaluated the exploitation potential of the SINTRA Port Use Case, particularly for safety, security and environmental monitoring applications. The developed capabilities in audio AI inference, sound localisation and multi-sensor data fusion are relevant to Sorama's existing smart city, smart mobility and smart stadium markets. In the next period, Sorama will continue validating these technologies in the port environment and assess their transferability to other ports and related markets in Europe and North America through its direct sales, VAR and strategic partner channels. | | | |
| Sensolus | sme | BEL | 6 PY |
| Sensolus prototyped an ad-hoc localization infrastructure within SINTRA: 10 Zone Anchors, vehicle trackers, and secure BLE tags developed with Sirris using lightweight cryptography for tag verification. These self-localizing, edge-optimized scanners run on battery or external power for high-frequency gate and trailer scanning. Smart cloud algorithms synchronize heterogeneous scanners for reliable location data, and a management system gives non-technical end-users one-click deployment with one-minute installation and diagnosis.<br><br>Sensolus targets existing customers and new prospects with low-value assets previously not viable to track: construction sites, pallet leasing, aerospace, industrial manufacturing, transport and logistics. A TCO below 1 EUR/month/asset over 5 years moves Sensolus down the asset pyramid, making low-value tracking economically viable. Positioned as low-cost tracking made simple and secure, it competes with RFID players on long battery life, no or limited wiring, end-to-end security, and easy adoption. Sold as recurring TaaS. Validated through lab tests, Malle, Rumst, Zedelgem and selected customers. | | | |
| Teleste | ind | FIN | 6 PY |
| Project enables Teleste to enhance situational awareness and video surveillance solutions further with AI and edge computing architectures and enhanced cyber security. In the project we are focusing in bringing situational awareness system into edge. We'll focus in developing architecture which allows robust and secure transmission and storage of video and other data in the moving vehicles and in the surrounding smart city infrastructures. The targeted solution also focuses on covering data governance and privacy aspects in the developed solution and proof of concept.<br><br>Project results shall reinforce Teleste's future offering and competence and thus increase turnover in the public safety domain.<br>Project results are commercialized in existing public safety market segment. Project results improve existing offering and address into new requirements, such as into ever tightening GDPR requirements and regulations | | | |
| Abloy Oy | sme | FIN | 4 PY |
| Our critical Infstructure (CI) business unit is focusing on critical infrastructure verticals such as telecom, energy, water, transportation, mining, oil and petroleum by offering mechanical, electro-mechanical and digital access control and locking solutions. Our customers are located globally e.g. in Europe, USA, Canada, LatAm, South-America, Africa, APAC. High security is at core in our business, as we're secure critical operations in society, sometimes in very challenging environments with increased crime rate. | | | |
| Citymesh | ind | BEL | 5 PY |
| Besides supplying our clients with ultra-reliable, high throughput networks, we also provide solutions on top of these networks, like AGVs, AUV's, Push-To-X, Climate sensors and others. These devices send out significant amounts of data, but usually work separately from each other. We believe strongly that by using multi-modal fusion we can leverage these devices that now work independent of each other by making them work together in order to make faster automated decisions, providing our clients with a more complete end-to-end solution.<br>With the increasing development and integration of semi-autonomous vehicles featuring remote operating capabilities within Flanders' largest industrial firms, such as BASF, there arises an opportunity to capitalise on this project. Leveraging the experience gained from remotely operating a robot dog, we can seamlessly extend our capabilities to implement other ground vehicles that can be operated remotely, including but not limited last-mile delivery vehicles.<br>We believe that offering such- | | | |
| SkyeBase | sme | BEL | 5 PY |

| | | | |
|---|---|---|---|
| SkyeBase offers a total solution to industrial customers in the petrochemical and maritime sectors (container and tank terminals, refineries). It combines (i) robotic drone inspections under a Drones-as-a-Service model and (ii) the iSPECT SaaS platform for AI defect detection and localization on digital twins. SkyeBase has a solid position in the Benelux, inspecting critical assets like STS cranes, piping and tanks. It also serves construction, energy and public infrastructure.<br><br>Market access rests on a partner network, agreements with notified bodies, ISO 9001 and VCA petrochemical accreditation, and strategic investment by Vinçotte Kiwa. The European LUC, extended with extra operational privileges, allows cross-border operations in all EASA member states. Additional BVLOS privileges were obtained in September 2026.<br><br>SkyeBase grows internationally through a new iSPECT yard surveillance module, multinational customers and partner resale. In Europe, port and airport surveillance demonstrators are ongoing in Finland, Spain (Valencia) and Greec | | | |
| KoçSistem Information Communications Services | ind | TUR | 4 PY |
| During this reporting period, exploitation prospects were further strengthened through the integration and validation of a multimodal anomaly analysis platform combining anomaly detection, open-vocabulary object recognition, depth reasoning, and spatial localization. The solution enables explainable detection of threats, crimes, and abnormal activities while providing contextual understanding and 3D positioning of relevant objects. These capabilities increase its applicability in public safety, airport monitoring, critical infrastructure protection, intelligent transportation, and smart facility management. Demonstrations and validation activities confirmed the operational feasibility of the approach, while the developed depth-aware and explainable AI capabilities provide clear differentiation from conventional video analytics solutions, supporting future commercialization and market adoption. | | | |
| Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş. | ind | TUR | 4 PY |
| Success of SINTRA project will give opportunity to develop new technologies to the market. Alpata Technology will get benefit from project results with building skills on Airport IoT based Anomaly Analyzer. Alpata Technology exploit results of SINTRA project with developing optimization solutions for industry, developing industrial software solutions and creating new projects. After exploitation process of project results, Alpata Technology will disseminate project results with optimizing products through different industrial needs. Project outcomes will be disseminated with attending demo days, web site blogs and conference procedings. | | | |
| SafeCity B.V. | sme | NLD | 2 PY |
| SafeCity BV already has a good relation with the harbors and airports in Belgium and the Netherlands, known as an innovator and expertise of the market. This knowledge is used in this Sintra project and the results of Sintra will be disseminated by SafeCity, and SafeCity will be the entrance to the market for the other partners of the project. SafeCity is mainly an innovation advisor for the logistic hubs (harbors, airports, industrial area's, transport companies) with the knowledge of safety and security.<br>Sintra will support SafeCity as an innovation advisor and will certainly give more work for the coming years. In 2025 SafeCity gave several presentations and lectures. The knowledge gained from the Sintra project is proving to be an added value for SafeCity's leads and prospects. SafeCity is increasingly positioning itself as a consultancy firm. | | | |
| Secapp Oy | sme | FIN | 3 PY |
| The role of sensors and IoT solutions is continuously increasing as organizations strengthen their preparedness and improve their ability to manage unexpected situations such as incidents, security threats, emergencies, and crises. Secapp plans to utilize the APIs and interfaces developed in the SINTRA project to complement its existing preparedness and incident management platform, which is provided as SaaS in Finland and North America, as well as through on-premise deployments globally. The utilization of these APIs will address customer- and segment-specific needs related to data collection, exchange, use, and storage, while the core Secapp platform itself remains unchanged.<br><br>The APIs and interfaces developed specifically within the SINTRA project enable secure incoming and outgoing data and event flows between the Secapp platform and external systems, sensors, and | | | |

| | | | |
|---|---|---|---|
| background platforms. From Secapp's perspective, these APIs constitute the primary technical outcome of the project and provide a complementary integration layer. | | | |
| Sensoan Oy | sme | FIN | 3 PY |
| Sensoan serves B2B customers in various industries, including e.g. power distribution and storage, intelligent buildings and environmental sensors. With the results of the project we can further enhance our offering in these sectors. Collaboration within the consortium opens new perspectives and creates networking opportunities internationally.<br><br>Sensoan, as part of the SINTRA project, is developing two innovative products that address critical needs in IoT connectivity and perimeter security: a dual-role gateway and a multi-sensor fence monitoring device.<br><br>Gateway<br>The gateway is designed to operate in two modes:<br>--Standard Gateway: Bridges a 2.4 GHz mesh network to LTE-M, ensuring secure and reliable data transfer to cloud or local servers.<br>--DECT NR+ Node: Functions as part of a self-organizing DECT NR+ mesh network, enabling ultra-reliable, low-latency communication and scalability for millions of devices.<br><br>This dual capability positions Sensoan uniquely in the market by offering redundancy and resilience. | | | |
| SIRRIS | res | BEL | 3 PY |
| Sirris plans to transfer the knowledge acquired in the context of the SINTRA project through appropriate new advisory services to help Belgian companies better acquire, aggregate & exploit multimodal data sources in view of prediction & planning through distributed machine learning techniques and privacy preserving and security measures. Sirris plans to offer these new services first to its member companies, and in a second phase to the broader Belgian industry. Furthermore, Sirris plans to disseminate the SINTRA project results towards both its member companies and the broader Belgian industry by performing dedicated awareness creation activities. Finally, Sirris intends to use the project results through follow-up national and industry-oriented R&D projects. | | | |
| Airobot | sme | BEL | 2 PY |
| Airobot would like to offer a cloud based solution based on a small, lightweight, automated drone in a box, which can easily be deployed. This solution will bring drone based security in reach of companies and organizations to protect their infrastructure in a cost effective way. When installed on a construction or stockpile site, the drone can also be used for measurements and stock-keeping (in combination with AiroCollect).<br><br>By integrating our current AiroLive solution with other security systems and interacting with the security business community, Airobot would like to open this new market and create a new business line. Today, Airobot can use commercially available drones from DJI and our own industrial drones, but would also like to expand it to other manufacturers. | | | |
| C-SITE | sme | BEL | 1 PY |
| Since 2016, C-SITE has been expanding to other types of clients and projects. This progression has been gradual. Initially, the focus was on similar types of building projects and construction companies. Presently, we have clients from all types of players in the construction and real estate industry, engaged in all kinds of construction projects. In other words, we nearly cover the entire B2B market of construction and real estate (AEC) . This also means that our business exposure on a specific type of project is limited in case there would be a downturn for a specific type of development, i.e. office buildings. | | | |
| Port authority | sme | FIN | 0 PY |
| Port of Kemi runs port facilities in the Kemi port in Northern Finland. In addition, it has several operators, with various types of market access globally. The largest operators at Kemi Port are: Kemi Shipping, BBLogistics, Chemec, Neste and Wibax Logistics. For example, Neste is the world's leading producer of sustainable aviation fuel, renewable diesel and renewable feedstock solutions for various polymers and chemicals industry uses. Neste uses port facilities worldwide, and therefore offers a direct market channel for SINTRA solutions tested in Port of Kemi. | | | |
| Port of Moerdijk | sme | NLD | 0 PY |

| |
|---|
| Port of Moerdijk provided scenario-based workflows for the security-industry and security management systems. In 2025 and 2026 we continued test this workarounds and provide other harbour-areas with our workflows and anomaly-based scenario's. We also created an extra scenariotype, made investigation on the scenario "burglary of truckcombinations" possible.<br>In 2026 we created scenariotypes for the harbour entrances (testing in fieldlab 3) |

## 3.2. Top 8 cumulative project achievements

| 1 | Exploitation | New system | Multi-modal AI-based incident detection and verification system for airport environments<br>Description | 1 |
|---|---|---|---|---|
| Summary | | SINTRA partners developed an integrated multi-modal incident detection and verification system combining IoT sensor anomalies, AI-based video analytics, smart CCTV infrastructure and spatial sensing. Alpata sensor outputs and ARD event detections are used as event triggers, while TAV Technologies provides the orchestration, video analytics, event correlation and incident-management layer. In cooperation with Inosens, CCTV smartization and camera-to-real-world coordinate mapping are being developed using LiDAR as a calibration reference, enabling detected events to be associated with their physical location and relevant camera views. The resulting architecture combines sensor evidence, computer-vision outputs and contextual AI analysis into a single explainable incident record for operator decision support. | | |
| Impact | | The achievement transforms isolated sensor and CCTV alarms into a unified and explainable incident-management approach. By correlating heterogeneous sensor events with camera analytics and spatial information, the system is expected to reduce manual camera monitoring effort, improve event verification, and support faster and more informed operator response in large-scale airport environments. The modular architecture can also be transferred to other critical-infrastructure domains requiring multi-sensor situational awareness. (quantification: Not yet applicable / To be quantified during final validation.) | | |
| Partners | | TAV Technologies, inosens, ARD GROUP, Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş. | | |

| 2 | Exploitation | New system | System to search-find-follow a suspect by a drone | 1 |
|---|---|---|---|---|
| Summary | | The system is able to detect a criminal activity by a static camera, record the appearance of suspects, and then invoke a drone that is able to search and reidentify them within the perimeter of the premises. When a suspect is re-identifed, the drone is following the suspect and reporting the suspect' coordinates to the dashboard. | | |
| Impact | | High (quantification: 100 pax) | | |
| Partners | | Eindhoven University of Technology, Avular Innovations B.V., ViNotion BV, Omines Internetbureau B.V., Port of Moerdijk | | |

| 3 | Dissemination | To customers | Creation of pilot: Fieldlab 3 at Port of Moerdijk | 1 |
|---|---|---|---|---|
| Summary | | Multi-modal sensors are installed at the river-entrance of the Port of Moerdijk (Fieldlab 3). Data is collected on vessels, humans and objects by static cameras and UAVs. AI models are trained on this data to detect the following activities: drug smuggling, immigrant trafficking, unauthorized boating, spilling to water, goods smuggling via small boats. | | |

| | |
|---|---|
| Impact | NA (quantification: 100 pax) |
| Partners | Eindhoven University of Technology, MantiSpectra, Avular Innovations B.V., ViNotion BV, Omines Internetbureau B.V., IQSight, Sorama B.V., SafeCity B.V., Port of Moerdijk |

| 4 | Dissemination | Publication | Article in De Telegraaf, main Dutch newspaper, about SINTRA | 1 |
|---|---|---|---|---|
| Summary | | The major Dutch newspaper published an article about the results of the SINTRA project: “Smokkelaars in havens straks kansloos door AI-tools”. The link: https://www.telegraaf.nl/lifestyle/tech/smokkelaars-in-havens-straks-kansloos-door-ai-tools/158609514.html | | |
| Impact | | Very high for dissemination (quantification: 3 mln readers) | | |
| Partners | | Eindhoven University of Technology, Avular Innovations B.V., ViNotion BV, SafeCity B.V., Port of Moerdijk | | |

| 5 | Exploitation | New system | Dual MCU architecture on sensor device | 1 |
|---|---|---|---|---|
| Summary | | We created dual MCU sensor system using Nordic Semiconductor's two radio modules from 3rd party vendor. This success lead to successful deployment of perimeter surveillance system in Port of Kemi. This also inspired to design embedded device based on this design that can be exploited further down the line on other use cases inside critical infrastructure as well. | | |
| Impact | | New device architecture for possible future systems and products. (quantification: We already have few interested customers to pilot the new device architecture.) | | |
| Partners | | Sensoan Oy | | |

| 6 | Exploitation | New system | Explainable AI-based closed-loop human risk management engine | 1 |
|---|---|---|---|---|
| Summary | | Hoxhunt researched and validated an automatic behavioral human-risk reduction engine: security events from heterogeneous third-party security tools are normalized into a vendor-neutral event vocabulary, mapped to individual behaviors, scored with explainable AI-based per-person risk assessment, and acted on automatically through AI-generated, individually targeted training and escalating interventions. This advances the state of the art, where human risk is assessed from phishing simulations alone and behavioral signals remain siloed in individual security tools. The results are already being exploited: the validated capabilities will be released as part of Hoxhunt's commercial human risk management platform before the end of 2026. | | |
| Impact | | The validated results reposition Hoxhunt to a human risk management platform provider, opening a new expansion revenue stream from 2027 and widening the addressable market. (quantification: Not applicable) | | |
| Partners | | Hoxhunt Oy | | |

| 7 | Exploitation | New system | SOTA Data fusion / visualisation platform for surveillance and monitoring purposes | 1 |
|---|---|---|---|---|

| | |
|---|---|
| Summary | We created a cloud based software platform where we combined several datasources into a single system, usable in any browser, to create advanced algorithms that can overlap different integrators and derrive insights that would otherwise be lost. We integrated: 3D model of the surveillance site, Advanced drone positioning and frustum visualisation system, AI detection systems for people tracking on drone footage, mapping the found AI persons of interest on the 3D model, sensor data, fixed camera feeds and their frustum, etc. |
| Impact | Not available yet due to being SOTA. (quantification: Not applicable) |
| Partners | SIRRIS, Macq, C-SITE, SkyeBase, Citymesh, Sensolus |

| **8** | **Human capital** | **Hiring at the project end** | **A new SW engineer was hired** | **1** |
|---|---|---|---|---|
| Summary | | Our contract to develop the firmware for a drone gimbal requires more effort to deliver a first release. New engineers are hired. | | |
| Impact | | More resources for growth (quantification: 5% growth) | | |
| Partners | | ViNotion BV | | |

## 3.3. Realised achievements

| Dissemination | Exploitation | Standardisation | New company | Patent | Human capital |
|---|---|---|---|---|---|
| Total: 29 | Total: 38 | Total: 0 | Total: 0 | Total: 0 | Total: 5 |

# 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

**1. Multi-Modal Detection and LiDAR-Assisted Person Localization**

During the reporting period, the airport use case advanced the integration of CCTV analytics with LiDAR-assisted spatial mapping and multimodal detection capabilities. Person and event detections from camera streams were associated with real-world coordinates through refined calibration and synchronization methods, while additional sensor information was incorporated to support cross-modal event interpretation. The resulting pipeline improved situational awareness and achieved approximately 90% localization accuracy under representative validation conditions at the TAV Technologies Innovation Hub.

**2. Perimeter Sensor Network**

The work introduced a modular and cost-efficient hardware platform using commercial components and custom elements, validated open-terrain mesh networking for perimeter-fence monitoring, and demonstrated wireless communication ranges of up to approximately 90 meters between nodes. PIR and accelerometer sensors were successfully tested for intrusion detection, while the trials also identified the future need for sensor fusion and ambient-light sensing to improve reliability. Over-the-air firmware updating was significantly improved and successfully demonstrated for gateways and sensor nodes, supported by enhanced diagnostic capabilities. In addition, a DECT NR+ sensor network was successfully demonstrated during a NATO exercise in the Turku archipelago, showing multi-kilometre communication, autonomous data collection by an unmanned surface vessel, integration with a national situational-awareness system, and strong potential for future long-range, autonomous, and dual-use monitoring applications.

**3. AI-Based Pedestrian Crossing Intent Prediction for Proactive Safety Monitoring**

A pedestrian intent prediction pipeline was implemented and refined to anticipate whether pedestrians will cross within a defined time horizon. The solution combines pedestrian detection, robust tracking and re-identification after occlusions, pose and motion-history information, and pixel-to-real-world coordinate mapping. An XGBoost-based classifier achieved the best results for predicting crossing up to 3 seconds ahead, while runtime optimisation increased the effective analysis rate from 5 to 11 fps, supporting progress towards real-time deployment.

**4. Full-cycle 24/7 Criminals' Multimodal Monitoring: Detection, Re-identification, Follow**

At this conclusive period of 2026, partners have integrated all the individual innovations, such as:

- AI anomaly detection and localization
- Re-identification of people from camera and drones
- Multi-modal data fusion for analysis (visual, IR, acoustics)
- Visualization dashboard with real-time event mapping (digital twin)
- UAV integration with IR and RGB gimbal
- Drug detection sensor
- Acoustic monitors
- Fusion of AIS and visual vessel detection

has been integrated into a single prototype for **full-cycle 24/7 Criminals' Multimodal Monitoring: Detection, Re-identification, Follow.** This system is now going to demonstrated at the European symposium Protection of Critical Infrastructure in Eindhoven, 5 October 2026 https://itea4.org/event-overview.html .

### 4.1.2. Top 4 next technical targets

| **1. Autonomous Camera-to-World Mapping with LiDAR Reference** |
|---|

The target is to automate the transformation of perspective CCTV observations into real-world coordinates by using LiDAR or other self-localising sensors as spatial reference sources. Deep-learning-based point generation and improved temporal alignment will be investigated to establish reliable pixel-to-location correspondences. The solution will be validated together with Inosens through queue-length and waiting-time estimation in representative airport gate scenarios at the TAV Technologies Innovation Hub.

| **2. AI Analysis of Kemi Seaport Data** |
|---|

The technical target is to **develop and validate an AI-based multimodal data analysis capability for the Kemi Seaport use case**, integrating heterogeneous sensor and surveillance data into the SINTRA platform to support automated anomaly detection, situational awareness, and operational decision-making. The platform will combine data from perimeter sensors, cameras, environmental measurements, network nodes, and other available sources, using standardized and secure data pipelines for preprocessing, synchronization, quality validation, and AI analysis. The modular SINTRA platform is designed to transform these surveillance feeds into higher-level knowledge through context-driven multimodal fusion and ultimately support a common situational picture for port stakeholders.

| **3. I-Based Pedestrian Crossing Intent Prediction for Proactive Safety Monitoring** |
|---|

Validate and optimise the pedestrian intent prediction pipeline on the target Macq camera hardware, including runtime benchmarking and further performance optimisation where required. Improve classification of challenging pedestrian behaviours, particularly the **"Waiting"** class, and further strengthen detection and pose estimation under occlusions. The target is to progress the current

pipeline towards robust real-time crossing-intent prediction under representative deployment conditions.

| 4. Full-cycle 24/7 Criminals' Multimodal Monitoring: Detection, Re-identification, Follow |
|---|

Improve the robustness of the prototype such that the demonstrations can be shown live in Port of Moerdijk.

### 4.1.3. Top 4 issues

| 1. Limited Flexibility for On-Site Data Collection |
|---|

***Details***:

A planned on-site data collection campaign had to be postponed several times due to adverse weather conditions preventing drone operations. Further rescheduling at the originally selected site was eventually no longer possible.

***Impact***:

The planned data collection at the original operational site could not be completed, limiting the possibility to collect and validate data in the originally targeted environment.

***Mitigation action***:

The consortium identified an alternative realistic testing environment and successfully conducted the joint data collection campaign there, allowing the planned data collection and subsequent technical activities to continue.

| 2. Lidar Assisted Pixel Location Mapping Calibration Issues |
|---|

***Details***:

Accurate transformation of CCTV pixel coordinates into real-world positions required more extensive camera–LiDAR calibration than initially expected, particularly due to perspective effects, reference-point matching and synchronization requirements.

***Impact***:

The issue increased the effort required for reliable spatial mapping and delayed the full automation of CCTV-to-world coordinate alignment, affecting the scalability of location-aware tracking across multiple cameras.

***Mitigation action***:

Camera–LiDAR datasets were collected using common reference points, and calibration, synchronization and pixel-to-world mapping methods were refined at the TAV Technologies Innovation Hub. The approach has significantly improved, while further automation and robustness testing are still ongoing.

| 3. Local Authority Approval and Operational CCTV Access Constraints |
|---|

***Details***:

Access to operational airport CCTV systems is subject to formal approval by local authorities and security bodies in Türkiye, which limited large-scale validation in a live airport environment.

***Impact***:

This restricted the possibility of testing the Türkiye use case with larger passenger populations and led to the final validation level being set at TRL 7 instead of TRL 9.

***Mitigation action***:

Validation activities were carried out at the TAV Technologies Innovation Hub, which provides real CCTV infrastructure and airport-representative spatial conditions. This enabled realistic system testing despite the access constraints at operational airports.

| 4. Regulators Permission for Drone Flights |
|---|

***Details***:

Currently, the Dutch authorities strengthen the control on drone flights in the restricted areas (our field labs in Port of Moerdijk are in such areas). At the same time, they keep bureaucracy and slow response at the same level. Obtaining a clearance requires 6 months. For Field lab 3 at PoM, we still have no clearance.

***Impact***:

We cannot demonstrate the drone reidentify-and-follow functionality of the SINTRA prototype in the Field lab 3 at PoM.

***Mitigation action***:

During demo, we will be re-identifying and following the suspects in the fields nearby Port of Moerdijk. In these fields, the drone flights are allowed.

### 4.1.4. Status of deliverables

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

The total planned number of deliverables in the project is 29. The original project plan included 30 deliverables; however, following the approved project updates, D2.1 and D2.4 were merged into a single deliverable, reducing the total number to 29. In addition, the former D2.5 was relocated under WP5 and is now reported as D5.7.

**[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, 22 deliverables were planned to be finalised according to the updated project plan. 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

D2.1 Data governance acquisition, sharing and access processes

D2.2 Ethical data handling guidelines report

D2.3 Cybersecurity measures implementation report

D4.1 Data governance protocol

D4.2 Data management plan

D4.3 Demonstrator reports

D4.4 Integration reports

D5.1 Public/internal website

D5.2 Dissemination and communication plan

D5.3 State-of-the-Art analysis

D5.4 Current and perspective business models

D5.5 Exploitation plan

D5.7 Platform deployment and maintenance manual

D6.1 Project and risk management plan

D6.2 Progress and quality assurance report 1

D6.3 Progress and quality assurance report 2

**[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, all 22 deliverables planned for completion by June 2026 have been finalised and uploaded to the ITEA Portal.

| Deliverable | Due date | Final version / upload | Status | Delay / clarification |
|---|---|---|---|---|
| D1.1 | May 2024 | Portal final upload date | Finalised | No delay |
| D1.2 | Aug 2024 | Portal final upload date | Finalised | No delay |
| D1.3 | Aug 2024 | Portal final upload date | Finalised | No delay |
| D1.4 | Aug 2024 | Portal final upload date | Finalised | No delay |
| D1.5 | Aug 2024 | Portal final upload date | Finalised | No delay |
| D1.6 | Nov 2024 | Portal final upload date | Finalised | No delay |
| D2.1 | May 2026 | Jun 2026 | Finalised | No delay, due date was updated from May to June 2026; merged with former D2.4 |
| D2.2 | Aug 2025 | Portal final upload date | Finalised | No delay |
| D2.3 | Aug 2025 | Portal final upload date | Finalised | No delay |
| D4.1 | Nov 2024 | Portal final upload date | Finalised | No delay |
| D4.2 | Nov 2024 | Portal final upload date | Finalised | No delay |
| D4.3 | May 2026 | Jun 2026 | Finalised | No delay, due date updated from May to June 2026 |
| D4.4 | May 2026 | Jun 2026 | Finalised | No delay, due date updated from May to June 2026 |
| D5.1 | Jun 2024 | Portal final upload date | Finalised | No delay |
| D5.2 | Sep 2024 | Portal final upload date | Finalised | No delay |

| | | | | |
|---|---|---|---|---|
| D5.3 | Nov 2024 | Portal final upload date | Finalised | No delay |
| D5.4 | Mar 2025 | Portal final upload date | Finalised | No delay |
| D5.5 | Aug 2025 | Portal final upload date | Finalised | No delay |
| D5.7 | Jun 2026 | Jun 2026 | Finalised | Former D2.5; relocated to WP5 and aligned with final platform deployment activities |
| D6.1 | Jan 2024 | Portal final upload date | Finalised | No delay |
| D6.2 | Nov 2024 | Portal final upload date | Finalised | No delay |
| D6.3 | Nov 2025 | Portal final upload date | Finalised | No delay |

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

No deliverables were delayed by more than two months during this reporting period. D2.1, D4.3 and D4.4 were rescheduled from May to June 2026 and completed within the reporting period.

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

During the reporting period, the SINTRA project progressed broadly in line with the updated project plan, with continued international collaboration across the technical work packages and use-case partners. Integration, validation and demonstration activities advanced across the airport and port-related use cases, while several project outputs were further consolidated. A Change Request was submitted to formally reflect updates to the deliverable structure and schedule, including the merger of D2.1 and D2.4, the relocation of the former D2.5 to WP5 as D5.7, and the rescheduling of D2.1, D4.3 and D4.4 from May to June 2026. These changes did not result in delays exceeding two months, and the overall project remains on track toward the final project phase.

### 4.2. Details of progress per Work Package

#### WP 1: Use cases, requirements & architectural specification

WP1 has already ended in 2025. The D1.6 architecture deliverable has been updated with the latest platform architecture decisions. The architecture and platform are being implemented in the other work packages.

### WP 2: Data governance & sharing: security, privacy protection & ethics

Work Package 2 (WP2) has been successfully completed, and all planned deliverables have been finalized:

D2.1: Data Governance, Acquisition, Sharing and Access, Privacy Protection, and Ethics

It combines regulatory requirements, stakeholder expectations, data quality principles and partner responsibilities, providing the foundation for controlled data acquisition, processing, sharing and access. The framework supports privacy protection, interoperability and trustworthy AI analysis across the consortium.

D2.2: Ethical Data Handling Guidelines Report

It defines principles and practical guidance for responsible data handling and AI use across SINTRA's applications. It addresses GDPR compliance, data ownership, access control, secure sharing and privacy-preserving techniques, while emphasizing transparency, fairness, accountability and human oversight. The report provides guidance for specific use cases, including port monitoring, and outlines monitoring, auditing and risk mitigation measures to support ethical and trustworthy deployment of the SINTRA platform

D2.3: Cybersecurity Measures Implementation Report

It provides guidance for assessing and managing cyber risks in sensor systems used in SINTRA's critical infrastructure applications. It reviews threats, vulnerabilities, risk assessment frameworks and security metrics. The report emphasises secure sensor selection, continuous monitoring and lifecycle risk management to protect data integrity, operational continuity and safety.

### WP 3: Multi-modal trustworthy AI analysis: anomalies, threats, crime

WP3 has been successfully finalized during the reporting period. In this period, efforts focused on finalizing WP3 activities and consolidating the results into four key deliverables completed and delivered in July and August. Deliverable D3.1 (Multi-modal data fusion and analysis report) documented the development of the SINTRA multi-modal data fusion and analysis framework, addressing the integration of heterogeneous sensing modalities and advanced fusion methods to enhance situational awareness and anomaly detection. Deliverable D3.2 (AI-based anomaly, threat detection development report) presented the AI-based anomaly and threat detection technologies developed across the project use cases, including the associated challenges, methodologies, and achieved results. Deliverable D3.3 (Robust and resilience of AI systems report) investigated the state of the art in trustworthy multi-modal AI, analyzing threats to AI systems and proposing the SINTRA Trustworthy AI Framework to improve robustness, resilience, and trustworthiness in critical infrastructure environments. Finally, Deliverable D3.4 3.4 (Adversarial attack prevention and mitigation report) reported on the techniques developed to protect AI systems against adversarial attacks, including poisoning, evasion, and Trojan attacks, thereby strengthening the security and reliability of the project's AI solutions.

### WP 4: Cross-coordination, visualisation, and demonstrators

During the first half of 2026, Work Package 4 made significant progress in consolidating the project's visual integration, demonstrator reporting, and evaluation preparations as SINTRA moves towards its final phase.

Task 4.2 (Visualization and demonstration) & Deliverable D4.3:

The Task 4.2 reporting phase has been successfully finalized with the completion and submission of D4.3 Demonstrator Report. This comprehensive report documents all tangible deliverables and user-level visual tools developed across the consortium's field labs (including the Port of Moerdijk, Belgian sites, Turkish airport pilots, and the Finnish Port of Kemi). The demonstrator tools showcase real-time multi-modal AI analysis, interactive operator dashboards, drone integrations, and situational awareness interfaces in practice.

Task 4.3 (Integration of AI systems with existing infrastructure) & Deliverable D4.4:
Task 4.3 was completed with the delivery of D4.4 Integration Report. This deliverable details the technical realization of the SINTRA "System of Systems" reference architecture across the various pilot instances. It proves the successful event-driven integration of WP2 data governance/cybersecurity mechanisms and WP3 multi-modal AI detectors (video, thermal, radar, acoustic, BLE) with the end-users' legacy infrastructures via Kafka/NATS event middleware.

Task 4.4 (System testing and evaluation) & Deliverable D4.5:
With the technical integration and demonstrator reporting finalized, work in Task 4.4 has actively commenced to prepare for the final evaluation report (D4.5 Evaluation Report). The report outline and evaluation template have been distributed to all consortium partners. Input is currently being collected from partners to validate both functional and non-functional project requirements (originating from WP1) as well as the quantitative Key Performance Indicators (KPIs), including detection accuracy, processing latency, false-alarm reduction, and GDPR compliance, across all use-case field labs.

## WP 5: Dissemination & exploitation

I. Dissemination:
- Article in the main Dutch newspaper about SINTRA: “Smokkelaars in havens straks kansloos door AI-tools” https://www.telegraaf.nl/lifestyle/tech/smokkelaars-in-havens-straks-kansloos-door-ai-tools/158609514.html
- Sara Abdulaziz, Abdulrahman Al-Abri, Giacomo D'Amicantonio, Egor Bondarev, Localizing to Debias: A Patch-Level Benchmark and Baseline for Weakly Supervised Spatial Anomaly Detection. European Conference on Computer Vision, ECCV 2026, Malmo, Sweden, September 2026.
- Sara Abdulaziz, Egor Bondarev. Auditing Frame-Level AUC in Weakly Supervised Video Anomaly Detection: Granularity, Resolution, and Scene Bias. European Conference on Computer Vision, ECCV 2026, Malmo, Sweden, September 2026.
- E Akdag, H Corporaal, Y Bondarau. MMTFL: Multi-Timescale Multi-Modal Feature Learning for Weakly-Supervised Anomaly Detection. Journal of Image and Graphics 14 (1), 96-107, 2026.
- Presentations of SINTRA results at SİU 2026 Conference on Signal Processing and Communications Applications:
o Artificial Intelligence and Dynamic Sensing for Security and Collaboration in Smart Environments
o mmWave Radar-Based Person Movement Detection for Airports
- Multiple LinkedIn posts, promo-movies at our https://sintra-ai.nl and https://sintra-ai.odoo.com/ websites

II. Presentations related to SINTRA in congresses, trade fairs:
a. At Düzce–Bolu R&D Project Market, 22 April 2026: INOSENS presented the AuraSens-r solution of radar-based crowd/person sensing algorithms.
b. Intersec, Dubai, UAE, January 12 - 14, 2026
c. ISCWest, Las Vegas, USA, March 23 - 27, 2026
d. FireSafety & Security Event, Den Bosch, Netherlands, April 15 - 16, 2026
e. BACOM Next Tech Day 2026, Bangkok, Thailand, May 27, 2026

III. Pilot projects:
a. Opened and exploited the Fieldlab 3 at the Port of Moerdijk: data collection and integration for vessel and water related criminal activities and surveillance
b. In the Fieldlab 3 at the Port of Moerdijk: added technologies for new scenarios, such as acoustic detection of anomalies and analysis of environmental pollution..
c. Further validation through customer acceptance testing and pilot activities for NATO border security applications in the Nordic countries.
d. Joint testing and data collection day in Zedelgem, 10 June 2026: 8 zone anchors plus BLE tags were deployed on site, together with two different drones and five static cameras. A full day of scan data was collected, and the dataset and site dashboard were shared with the Belgian consortium.
e. GOSB Teknopark: field data collection and system validation were carried out under different physical conditions, following privacy-by-design and local-edge data processing principles.
f. Additional validation activities were also coordinated within Use Case 1 through system integration, data collection, and algorithm verification workflows.
g. TU/e validation activities: radar hardware and integration guidance were provided to TU/e. Radar data were collected for several human-motion scenarios and used to validate and fine-tune INOSENS's 5D clustering/tracking algorithms.

IV. Discussions/presentations with municipalities, ports, customers and PAs:
a. Meetings with authorities inland harbours in Germany and The Netherlands
b. Promoting a SINTRA symposium among customers on October 5, 2026.

V. Deployed prototypes/products:
- AuraSens-r radar-based sensing demonstrator: deployed in field/test environments and demonstrated live for crowd/person sensing and spatial analysis.
- SINTRA 3D visualisation demonstrator: an Apple Vision Pro-based AR/MR application was developed to visualise mmWave radar point clouds interactively on-device and allow real-time interaction with sensing algorithms.
- High-volume orders of thermal cameras for border control applications.
- Continued development of the Zone Anchor infrastructure of Sensolus (battery-powered and externally powered scanners, cloud location inference, remote deployment diagnostics and firmware management), now under test with selected customers outside the pilot sites.
- Into airport MS: HOLMESVAD/Holmes-VAU framework customized with automatic prompts and confidence scoring
- Deployment-ready video anomaly detection tool with a web interface

- NER + SAM pipeline for anomaly localization

VI. New sub-systems integrated:
a. Sensolus asset-tracking data was integrated as a data source into the Belgian data fusion/visualization platform, where it can be combined with the 3D site model, drone and camera feeds, and AI detections. The data collected during the Zedelgem testing day was also integrated into the platform.

## WP 6: Project Management

During this reporting period, WP6 activities focused on maintaining coordinated execution during the final phase of the SINTRA project, consolidating project-level reporting, managing required project updates, and preparing the consortium for final validation and review activities. Particular attention was given to cross-WP coordination, deliverable alignment, Change Request preparation, partner reporting follow-up, and ensuring consistency between the technical progress achieved and the information reflected in the ITEA Portal.
Regular consortium coordination continued through weekly project leader meetings, national coordination meetings, and dedicated technical discussions involving the relevant work packages. These meetings were used to monitor technical progress, discuss integration dependencies, follow open actions, and coordinate activities required for the final project phase. Project documentation, meeting outputs, reporting templates, and updated planning information continued to be maintained through the shared digital collaboration environment.
Task 6.1 – Project Management and Coordination:
Project management activities concentrated on coordinating the final implementation and reporting period across the consortium. Particular effort was devoted to aligning partner contributions for the Periodic Progress Report, monitoring project-level deadlines, and coordinating the preparation of the final review. In parallel, several project structure updates were reviewed and consolidated in the ITEA Portal, including deliverable reallocations, timing adjustments, merging of related deliverables, and confidentiality updates. These changes were coordinated through the Change Request process to ensure consistency between the approved project plan, portal information, and actual technical implementation.
The management team also maintained close communication with WP leaders and consortium partners to resolve reporting-related issues, follow pending inputs, and ensure that required project information was submitted consistently. Coordination activities increasingly focused on completion readiness, integration maturity, demonstration planning, and alignment of technical achievements with exploitation and business objectives.
Task 6.2 – Risk Management:
Risk management activities focused on risks associated with final technical integration, validation readiness, reporting completeness, partner dependencies, and schedule alignment during the closing phase of the project. Existing risks were regularly reviewed in light of technical progress, while new risks related to final demonstrations, deliverable dependencies, and timely completion of partner contributions were monitored.
Task 6.3 – Excellence Assurance and Control:

Quality assurance activities during this period focused on the consistency, completeness, and maturity of project outputs ahead of the final project stage. Deliverables and reporting inputs were reviewed with particular emphasis on alignment between reported technical achievements, project objectives, KPIs, and the approved project plan. Cross-partner review was applied where deliverables depended on contributions from multiple technical work packages.
Task 6.4 – Progress Reporting and Project Deliverable Tracking:
Progress monitoring and deliverable tracking continued throughout the reporting period using the consolidated project tracking approach. Deliverable status, deadlines, dependencies, partner inputs, and project-level reporting requirements were regularly monitored and communicated to the consortium.
During this period, particular effort was devoted to preparing and coordinating the Periodic Progress Report and ensuring that partner contributions were collected and validated. Necessary updates to the project plan were also consolidated through the Change Request process, including the transfer of D2.5 to WP5 as D5.7, revised delivery dates for selected deliverables, the merging of D2.1 and D2.4, and confidentiality updates for D3.1–D3.4.
Overall, WP6 ensured continued management control during the final project phase, supported timely reporting and project-plan alignment, and provided the coordination framework required for final technical validation, final review preparation, and transition toward exploitation and project closure.

## 4.3. Per partner progress during the reporting period

### 4.3.1. Partners' main contribution and effort

| Partner | Planned effort (Project start~ end of reporting period) | Actual effort (Project start ~ end of reporting period) | Contact |
|---|---|---|---|
| ViNotion BV | 7.89 | 8.99 | Egbert G.T. Jaspers |
| | Main contributions during the reporting period:<br>We designed, implemented and ported a multi-sensor fusion algorithm for object detection on the Drone gimbal of the Avular drone. This systems was published on a conference. In addition, a novel single object tracking algorithm was designed, implemented and ported and is ready for validation. | | |
| | Discrepancy explanation:<br>The required R&D effort was originally underestimated. | | |
| Eindhoven University of Technology | 7.42 | 7.40 | Egor Bondarev |
| | Main contributions during the reporting period:<br>We have developed the following innovative AI models: 1. Re-identification of people in both CCTV and Drone views. 2. Fusion of thermal and RGB videos for robust detection of anomalous behaviour. 3. Detection of behaviour anomalies from UAV imagery. 4. Detection of hiding people in thermal imagery. | | |
| | Discrepancy explanation:<br>There are no discrepancies | | |
| MantiSpectra | 5.89 | 5.89 | Peter VISSER |

| | | | |
|---|---|---|---|
| | Main contributions during the reporting period:<br>Work was done to increase the sensitivity of our sensors, as well as firmware of the electronic boards | | |
| | Discrepancy explanation:<br>n.a. | | |
| KoçSistem Information Communications Services | 3.38 | 3.38 | Aylin Yorulmaz |
| | Main contributions during the reporting period:<br>Development and validation of a multimodal, explainable anomaly analysis framework integrating video anomaly detection, open-vocabulary object recognition, depth reasoning, and spatial localization. Scientific contributions were consolidated through dataset analyses, performance evaluations, system demonstrations, and dissemination via academic publications and conference presentations. | | |
| | Discrepancy explanation:<br>None | | |
| ARD GROUP | 4.57 | 4.87 | Arda Ödemiş |
| | Main contributions during the reporting period:<br>During this period, integration activities with TAV Technology were carried out, covering data acquisition and delivery of analytical outputs. Data preparation and annotation processes were improved, while event detection, heatmap generation, and AI model development activities continued. Experimental studies were also conducted to improve system reliability, performance, and operational applicability. | | |
| | Discrepancy explanation:<br>- | | |
| Port of Moerdijk | 0.25 | 0.25 | m.vandenberg@portofmoerdijk.nl<br>van den Berg |
| | Main contributions during the reporting period:<br>- installation fieldlab 3 (Roode Vaart) with 8 camera's and 5 microphones (2 underwater)<br>- testing-sessions fieldlab 3 and fieldlab 1.<br>- realisation fibre-connections with fieldlab 3 and new internetconnections<br>-introduction mobile monitoring device surveillance (Genetec)]<br>- using anomaly-profiles Sintra for Logistiek Park Moerdijk | | |
| | Discrepancy explanation:<br>none | | |
| SafeCity B.V. | 1.80 | 2.10 | Jan Otten |
| | Main contributions during the reporting period:<br>Talking, calling, visiting end-users and project-partners. Also police and harbour authorities. | | |
| | Discrepancy explanation:<br>More time needed to bring end-users together. Public-private partnerships are not a given; they require considerable powers of persuasion and discussions regarding the benefits of collaborating with researchers. | | |
| Hoxhunt Oy | 14.77 | 17.42 | Pyry Åvist |
| | Main contributions during the reporting period:<br>Research and development of the SaaS human risk analysis, mitigation and visualisation platform continued, maturing into validated capabilities: multi-source behavioral data fusion via vendor-neutral event vocabulary, explainable AI-based risk scoring, and closed-loop automated interventions. Hoxhunt has also contributed to the work packages and Finnish Port Use Case with Finnish partners. | | |

| | | | |
|---|---|---|---|
| IQSight | 8.35 | 8.35 | Ildiko Suveg |
| | Main contributions during the reporting period:<br>During the reporting period, work continued on thermal IQ to enhance visibility and detection performance, supported by real-world data collection using a multi-modal field-lab setup. The focus of this period shifted toward finalizing the WP3 deliverables and completing the preparations for the project demonstrators, which showcase the project's key results. | | |
| Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş. | 3.63 | 3.63 | Murat Sağlam |
| | Main contributions during the reporting period:<br>The sensor anomaly detection engine was moved to a two-stage contextual architecture and validated on the live sensor stream in the field, with false-alarm and fault-capture rates measured. Anomaly events were aligned with the consortium common event model to trigger camera-based visual verification. | | |
| | Discrepancy explanation:<br>No discrepancies were identified during the reporting period. | | |
| University of Jyväskylä | 12.44 | 4.22 | Markus Sihvonen |
| | Main contributions during the reporting period:<br>WP2 was successfully completed.<br>Leadership of Task D3.3 was successfully concluded, and the associated deliverable was completed. Deliverables D3.1, D3.2, and D3.4 were completed. The data collection platform was installed at Kemi Seaport. The AI platform was installed in the SINTRA laboratory and is ready for model training | | |
| | Discrepancy explanation:<br>The project started one year later than originally planned, and we experienced technical challenges in developing the sensor platform for data collection at the Port of Kemi. These challenges have now been resolved and we can focus threat analysis fully from now on. | | |
| SIRRIS | 2.52 | 2.62 | Farhad Aghili |
| | Main contributions during the reporting period:<br>WP2: Further progressed the visual privacy tool and integration activities. Continued CRA for the BLE-based ecosystem.<br>WP3: Implemented and evaluated AI components for pedestrian action recognition and crossing-intent prediction, object tracking, and RGB/IR alignment. Progressed integration and validation of AI components using collected data in Zedelgem for the BE platform(WP4-5). | | |
| Avular Innovations B.V. | 5.93 | 5.17 | Gino Van der Zijde |
| | Main contributions during the reporting period:<br>Development was focused on completing waypoint-following behaviour and releasing the first version of this feature. In parallel, payload control and streaming functionality have been been finalised. Preparations have also been made for integration with Vinotion software and the Omines dashboard, ensuring the developed functionalities are ready for integration & testing. | | |
| | Discrepancy explanation:<br>With the project in its last months, the efforts have increased to realize the project goals and planned effort before the project end date. | | |
| Sensolus | 5.20 | 5.20 | laurence claeys |
| | Main contributions during the reporting period:<br>Cybersecurity work with Sirris continued through risk analysis, threat | | |

| | | | |
|---|---|---|---|
| | modelling, SBOM, ... The secure beacon was validated end-to-end and TaaS model validation progressed. Zedelgem joined Malle and Rumst as a third pilot: zone anchors, tags and sensors deployed on the joint testing day, data integrated into the BE Port Platform. | | |
| Macq | 5.01 | 5.09 | Geert Vanstraelen |
| | Main contributions during the reporting period:<br>Continued data collection.<br>More accurate camera calibration, timestamping and FoV monitoring.<br>New modules in the Macq Mobility Manager M3 that are based on too long or to short zone presence. Integration of Clickhouse to access parquet files.<br>Exploitation of the rail way use case with stakeholders. | | |
| | Discrepancy explanation:<br>On track | | |
| C-SITE | 1.36 | 1.23 | Jelle Stuyvaert |
| | Main contributions during the reporting period:<br>C-SITE participated in the SINTRA Belgian Data Collection Day, downloaded, processed and supplied footage and supporting data, and contributed to project meetings and discussions. | | |
| | Discrepancy explanation:<br>Cumulative actual effort reached approximately 1.23 PY, compared with the planned 1.36 PY. Effort during this reporting period was lower than anticipated, with activities focused on data collection, footage processing and project meetings within the reduced scope approved by VLAIO. | | |
| Koçtaş Yapı Marketleri Tic. A.ş | 7.36 | 7.00 | Anıl Efe Çiftçi |
| | Main contributions during the reporting period:<br>Koçtaş developed camera based human and product detection, tracking, pose based anomaly analysis, dashboard and alert components for the retail fraud use case. Event rules and thresholds were refined through testing. A time based camera and POS matching model was defined, applying data minimisation, controlled access and human oversight principles. | | |
| | Discrepancy explanation:<br>Actual cumulative effort is 7.00 PY compared with 7.32 PY planned. The difference reflects phased execution of POS integration and end to end validation activities. Project scope and schedule remain unchanged. Remaining integration, testing and validation work continues within the approved plan and planned project period without affecting project objectives. | | |
| SkyeBase | 4.17 | 4.22 | Tom Daniëls |
| | Main contributions during the reporting period:<br>SkyeBase implemented data fusion pipelines integrating drone data with other data sources, and deployed the WP3 AI workflow in the joint PoC platform. SkyeBase continued design, research and development of the joint PoC platform architecture, advancing iSPECT yard surveillance beyond the current state of the art in multi-source situational awareness. | | |
| | Discrepancy explanation:<br>no significant discrepancy | | |
| Sensoan Oy | 2.40 | 1.12 | Kari Petteri Malmivirta |
| | Main contributions during the reporting period:<br>Sensoan's work focused on two SINTRA products: a gateway connecting mesh networks to LTE-M and supporting DECT NR+, and a fence sensor combining movement and acoustic monitoring. These developments support Sensoan's goals in resilient IoT connectivity and perimeter security. | | |

| | | | |
|---|---|---|---|
| | Discrepancy explanation:<br>Actual effort was below plan due to resource shortages late last year and the ongoing acquisition, which delayed project activities. The Finnish consortium joined the project later, creating an initial lag. Sensoan's project resourcing has since improved, enabling more consistent progress in the coming period. | | |
| TAV Technologies | 11.44 | 11.32 | Talha Koc |
| | Main contributions during the reporting period:<br>TAV Technologies advanced its event-driven AI video analytics by integrating object detection, anonymous tracking and multimodal AI for operational incident analysis. In parallel, camera–LiDAR calibration and synchronization studies were conducted to map CCTV pixel locations to real-world coordinates, supporting smarter camera selection and location-aware tracking. | | |
| | Discrepancy explanation:<br>The minor discrepancy between planned and actual effort is due to small variations in the timing and duration of technical activities during the reporting period. The overall effort remained closely aligned with the project plan, with no significant deviation in scope or responsibilities. | | |
| Teleste | 4.80 | 3.44 | Jani Väre |
| | Main contributions during the reporting period:<br>Work on WP2, WP3 and WP4, togerher with finnish consortium. | | |
| | Discrepancy explanation:<br>Some delays due to organizational changes. No impact on the project. | | |
| Abloy Oy | 3.38 | 0.82 | Jesse Juurelma |
| | Main contributions during the reporting period:<br>ABLOY contributed domain expertise, operational requirements, and validation activities. During the reporting period, a major focus was the preparation and deployment of the SINTRA pilot installation at Kemi Port, including stakeholder coordination and practical support for pilot execution. | | |
| | Discrepancy explanation:<br>The effort spent by ABLOY was lower than planned because our role in the project focused mainly on providing data, operational insights, and validation feedback rather than conducting active software development. Consequently, the actual workload required from ABLOY was lower than originally estimated in the project plan. | | |
| Omines Internetbureau B.V. | 4.91 | 4.90 | Niels Keurentjes |
| | Main contributions during the reporting period:<br>Implemented dashboards, central data exchange environments, coordinated data exchange and interoperability with project partners, implemented abstract data exchange portals for connecting to Rovers and Drones, external data connectors such as AIS and governmental open data. | | |
| Airobot | 1.75 | 0.00 | Jan Leyssens |
| | Main contributions during the reporting period:<br>Main contributions during the reporting period:<br>Airobot has formally withdrawn from the project as of 2025. | | |
| | Discrepancy explanation:<br>Main contributions during the reporting period:<br>Airobot has formally withdrawn from the project as of 2025. | | |
| inosens | 4.80 | 3.07 | Ismail Uzun |
| | Main contributions during the reporting period:<br>During the reporting period, INOSENS advanced the mmWave radar-based | | |

| | | | |
|---|---|---|---|
| | human detection and tracking solution for the airport use case. A dual-radar integration was developed to reduce occlusion effects and improve tracking continuity. The clustering, tracking, real-time processing, and secure WSS/JSON data transfer pipeline was further improved for SINTRA platform integration. | | |
| | Discrepancy explanation:<br>INOSENS will spend more time in integration part then previous terms. | | |
| Jyväskylän ammattikorkeakoulu | 4.50 | 1.80 | Aimo Pellinen |
| | Main contributions during the reporting period:<br>The Sintra Kemi-harbour demonstration in RGCE cyber range has been progressed through threat scenario development, AI capabilities, implementation, SINTRA architecture integration and OpenZiti security. Research activities advanced, establishing a strong foundation for integration, AI and further development. | | |
| | Discrepancy explanation:<br>The actual effort was lower than planned because the main project activities and related workload are scheduled to take place in 2027. Therefore, a larger share of the planned effort will be allocated to 2027. | | |
| Citymesh | 3.73 | 3.73 | Noa Lambert |
| | Main contributions during the reporting period:<br>Citymesh facilitated the organisation of the Belgian consortium test days, provided infrastructure, collected data, implemented and tested the research work done in the sintra project, namely the privacy preserving fragile watermarking. | | |
| 2NS Cybersecurity Oy | 5.50 | 5.50 | Juho Ranta |
| | Main contributions during the reporting period:<br>2NS contributed to the analysis of potential AI-related attack vectors and security threats. The partner also worked on concepts for enhanced security monitoring and threat analysis by combining vulnerability information from multiple sources. | | |
| Port authority | 0.25 | 0.25 | Markku Juhani Rautio |
| | Main contributions during the reporting period:<br>During this reporting period, Port of Kemi continued to support the validation of the SINTRA solutions in a real port environment and contributed operational knowledge from the Port Use Case. The project results are being assessed in terms of their applicability to port security, situational awareness and critical infrastructure. | | |
| Secapp Oy | 2.43 | 2.43 | Timo Harju |
| | Main contributions during the reporting period:<br>Secapp contributes its expertise in preparedness, incident management and secure system integration. Its main role is to develop and validate APIs and interfaces that connect the Secapp platform with external sensors, systems and background platforms, enabling secure information exchange and supporting the integration of SINTRA solutions into operational incident management. | | |
| Sorama B.V. | 5.72 | 5.72 | Thomas Willems |
| | Main contributions during the reporting period:<br>Sorama contributed to the Port Use Case through the development and evaluation of acoustic sensing and audio AI capabilities for safety, security and environmental monitoring. The partner also worked on sound localisation and the integration of acoustic information with other sensor data to support improved situational awareness. | | |

### 4.3.2. Actual vs. planned effort overview

| Report | Planned effort up to reporting period (PY) - total: 184.24 PY | Reported actual effort up to reporting period (PY) |
|---|---|---|
| 2026 Semester 1 | 157.50 (85% of total) | 141.13 |
| 2025 Semester 2 | 130.75 (71% of total) | 107.55 |
| 2025 Semester 1 | 95.48 (52% of total) | 76.31 |
| 2024 Semester 2 | 60.22 (33% of total) | 41.62 |
| 2024 Semester 1 | 31.78 (17% of total) | 19.12 |

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

**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.

Following the previous STG remarks, the deliverable structure, due dates and document status were reviewed and updated in the ITEA Portal. In particular, D2.1 and D2.4 were merged into a single deliverable, the former D2.5 was relocated under WP5 and is now reported as D5.7, and the due dates of D2.1, D4.3 and D4.4 were updated from May to June 2026.

The status of all deliverables due up to the end of the current reporting period has been clarified in this PPR, including the updated due dates, finalisation status and the reasoning for the restructuring. The corresponding updates can be verified in the Work Package deliverable lists in the ITEA Portal and in the Project Action List under Management. A Change request was submitted on 15.09.2026 for those minor updates.