2025-H1 Project Progress report

SINTRA

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

Edited by: All Consortium Partners

Date: September 29, 2025

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: 186.8 PY	Costs: 19.6 M€
Time frame	Start: 01-12-2023	End: 30-11-2026 (36 months)

Coordinator

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

Project Status

Latest FPP	Change Request (11-03-2025)
Latest PPR	2024 Semester 2
Latest Review	SINTRA #1 (a.m.) (15-01-2025)
Upcoming Review	SINTRA #2 (a.m.) (29-01-2026)
PCA status	PCA has not been signed yet

Consortium

Country	Funding Status	National Coordinator (Company)	Total Effort (PY)	List of Partners
Belgium	Funded (Y)	Farhad Aghili (SIRRIS)	26 PY	Airobot, C-SITE, Citymesh, Macq, Sensolus, SIRRIS, SkyeBase
Finland	Funded (Y)	Markus Sihvonen (University of Jyväskylä)	59 PY	Abloy Oy, Hoxhunt Oy, Jyväskylän ammattikorkeakoulu, Port authority, Secapp Oy, Second Nature Security Oy, Sensoan Oy, Teleste, University of Jyväskylä
The Netherlands	Funded (Y)	Egor Bondarev (Eindhoven University of Technology)	56 PY	Avular Innovations B.V., Bosch Security Systems B.V., Eindhoven University of Technology, 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
BLE	Bluetooth Low Energy
CCN	Convolutional Neural Network
CCTV	Closed-Circuit Television
Esora	Electronic Specific Operations Risk Assessment
EU	European Union
F&B	Food &Beverage
GDPR	General Data Protection Regulation
IoT	Internet of Things
IR	Infrared
KPI	Key Performance Indicator
KVKK	Kişisel Verilerin Korunması Kanunu - Turkish Personal Data Protection Law
mmWave	millimetre-Wave
RF	Radio Frequency
RGB	Red, Green, Blue
RNN	Recurrent Neural Network
SINTRA	Security of Critical Infrastructure by Multi-Modal Dynamic Sensing and Artificial Intelligence
SORA	Specific Operations Risk Assessment
UAV	Unmanned Aerial Vehicle
UGV	Unmanned Ground Vehicle
VR	Virtual Reality
WP	Work Package

Table of contents

1. Project one-page description

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

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

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

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

The benefits of the SINTRA platform will be demonstrated on four critical infrastructure types (use-cases): airports, harbours, construction sites, and shopping centers. With contributions from Netherlands, Turkey, Belgium, Finland, the SINTRA consortium is composed of partners that cover the full market value chain of research centers, sensor/data providers, platform, and service providers, where each country use-case is supported by one or more end-users. The consortium carefully balances the scale and impact of large industrial partners providing the platform and service

integrations with the in-depth expertise of academic institutes and the innovative power of selected SMEs. The project will actively engage with citizens, authorities, and external stakeholders to stimulate acceptance, validate scalability, and maximise the impact.

2. Project overall status

2.1. Top 4 overall targeted innovations

1. AI-Powered Anomaly Detection & Behaviour Detection

Main contributors: All partners

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

Current CCTV and rule-based systems can only flag predefined events (e.g., fence crossing, object left behind) and fail in complex, dynamic contexts. SINTRA advances this by combining deep learning (CNN, RNN) with behavioural analysis for detecting subtle and composite anomalies (e.g., smuggling, fights, theft). SINTRA integrates advanced AI models for anomaly detection using multi-modal data from cameras, IoT sensors, RF signals, and mmWave radars. AI techniques, including deep learning and video analytics, enhance security by identifying threats such as unauthorized access, violence, and cyber risks in airports, ports, and critical infrastructures. Recent results include real-time object detection, human-pose based fraud detection, and spatial anomaly localization.

2. Multi-Modal Sensor Fusion for Robust and Smart Surveillance

Main contributors: All partners

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

Traditional surveillance relies on single-modality sensors, leaving blind spots. SINTRA integrates acoustic (e.g., gunshot or tamper detection), visual (RGB/IR), radar, lidar, and multispectral sensors into a unified pipeline. Acoustic sensors detect sound waves and are used in various security applications, including gunshot detection, intrusion detection, and environmental monitoring. Visual sensors, such as CCTV cameras, provide critical visual data for surveillance. Radar sensors are utilized for their ability to detect objects and measure their speed, distance, and direction. Microwave radar sensors utilize high-frequency radio waves to detect objects in the surroundings using electromagnetic waves. Multispectral sensors capture data across multiple wavelengths, enabling the analysis of material properties and conditions. LiDAR sensors provide high-resolution 3D mapping, crucial for terrain analysis and object detection. Field labs at Port of Moerdijk have validated cross-sensor registration and acoustic-thermal fusion, with prototypes for maritime acoustic sensing now under testing.

3. Edge and Federated AI for Real-Time, Privacy-Compliant Decisions

Main contributors: All partners

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

Centralized cloud analytics often suffer from latency and GDPR/KVKK challenges. SINTRA implements edge and federated AI, processing data at source nodes (cameras, BLE scanners, UAVs) while preserving privacy via anonymisation and lightweight cryptography. Compared to the State-of-the-Art (IoT edge gateways with basic analytics), SINTRA enables advanced AI inference and cross-site learning without raw data transfer. This reduces response times and ensures compliance. The fusion of

multimodal sensor data provides a comprehensive security landscape, reducing false alarms and improving response accuracy. Advanced analytics enable real-time data processing on edge devices, ensuring rapid decision-making. With cybersecurity measures and privacy-aware data handling, the innovation provides an intelligent, connected environment for enhanced safety, efficiency, and automation in high-risk infrastructures.

4. Autonomous and Collaborative Aerial/UGV Surveillance

Main contributors: All partners

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

Existing drone/UGV solutions are often siloed, requiring manual control and lacking integration with multi-sensor AI. SINTRA introduces autonomous UAV/UGV fleets integrated with AI-driven detection and cross-border data sharing. Novel contributions include real-time object detection on UAVs, collaborative UAV-UGV demos in Belgium, and semi-autonomous drone surveillance flights under LUC certification. Compared with current commercial drone platforms (DJI, Parrot) limited to video feeds, SINTRA's approach provides fully integrated anomaly detection and secure inter-partner data exchange.

2.2. Top 4 overall targeted business impacts

1. Enhanced Security and Anomaly Detection at Airports

Short description: The project will introduce AI-driven, multi-modal anomaly detection to improve security at airports. AI-powered, multi-modal anomaly detection will reduce security breaches and operational disruptions in airports by enabling real-time detection of threats like unauthorized access, unattended baggage, and suspicious behavior.

Main contributors: TAV Technologies, Koçsistem, Alpata

Market / competitors:

The primary market includes international and regional airports, aviation security agencies, and government regulatory bodies. Competitors include Thales, SITA, and Honeywell, who offer advanced but largely siloed security systems. SINTRA differentiates by providing a scalable, multi-sensor, AI-driven solution with stronger real-time integration and higher detection accuracy.

2. AI-Powered F&B Safety and Surveillance

Short description: Introduction of AI-based monitoring in airport food & beverage (F&B) areas to enforce hygiene compliance and detect contamination or tampering risks, enhancing both safety and trust for passengers.

Main contributors: Koçtaş, İnosens, ARD

Market / competitors:

The market includes airport F&B vendors, global catering firms, and regulators. Competitors like NEC and Bosch provide generic surveillance solutions, but few address real-time hygiene and tampering risks in high-traffic airport settings. SINTRA positions itself as a dedicated compliance solution tailored to operational and safety needs in F&B.

3. Cross-Infrastructure Security & Compliance Platform

Short description: The SINTRA project delivers cutting-edge AI-driven compliance and anomaly detection platform for airports, ports, construction sites, and rail networks. By integrating advanced sensor fusion, real-time video analytics, and secure data governance, the platform ensures proactive threat detection, privacy compliance, and operational integrity. With features like AI-powered anomaly detection, automated access control, and federated learning for ethical AI, SINTRA strengthens resilience against security threats while maintaining regulatory compliance, such as GDPR.

Main contributors: All partners

Market / competitors:

Target customers include municipalities, law enforcement, and infrastructure operators. Competitors like Motorola Solutions and Dahua focus on AI surveillance but lack strong privacy-preserving features. SINTRA aims to fill this gap with GDPR-compliant, federated AI governance models, providing a market edge in “ethical AI” for security.

4. Smart Surveillance for Ports & Construction Sites

Short description: Deployment of AI-enhanced monitoring at ports, railways, and construction sites to detect smuggling, theft, and hazardous activities. This reduces losses, ensures compliance, and strengthens critical infrastructure protection.

Main contributors: Belgian, Dutch, Finnish partners

Market / competitors:

Governments, private port operators, and security providers are key markets. Competitors like Hikvision, Axis, and Genetec dominate with CCTV-based systems. SINTRA offers a differentiated value by combining multi-modal sensing (thermal, video, RF, mmWave) with real-time risk analysis, enabling earlier detection of smuggling and cargo theft.

2.3. Top 4 overall project KPIs

	Initial value	Targeted value	Current value
1.Threat detection success of CCTV Analyzer compared to alternatives	Initial value for V 0.0 is taken as %0.	min 95%	100% (continuous monitoring)

A reference video footage was recorded to measure and make comparison for versions. This reference video footage comprises: Congregating, removed object, fall, graffiti, direction violation, abnormal behaviour, running, suspicious meeting, fighting.

2. Reduction of missed anomaly/threat rate	100%. At the time of the beginning of the project 2023, no industrial anomaly detection systems were installed at any harbour control rooms.	20%	60%

The event records kept by the control room operators at the harbour will be compared with the system output.

3. Amount of detectable complex crime-related anomalies	1 anomaly type: Fighting (Violence)	3 anomaly types: Drugs trafficking, people smuggling and cargo thievery. Plus: 7 public safety threats	Current: 0/2 (violence and object throwing)

Actors physically play the anomalies in the field lab of Port of Moerdijk, and the detection results are assessed.

4. Visual privacy enhancement	No visual data privacy	Protecting privacy sensitive image/video content while achieving both high data capacity (minimum 3 BPP) and Image/Video quality (PSNR= above 40 dB)	PSNR=44.23, 6BPP for cover, 2BPP for watermark

Capacity: Measure the average bits per pixel (BPP) capacity for embedding encrypted data within images/videos. Quality: Measure the Peak Signal-to-Noise Ratio (PSNR) of images/videos before and after embedding.

2.4. Top 4 overall risks

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

Avoidance action:

The integration of various systems and the handling of sensitive data, especially in an airport and in harbour setting, can lead to data breaches or unauthorized access if not properly secured. Legal experts are to be engaged early in the process to ensure full compliance with GDPR and other relevant privacy regulations. Regular audits of data handling processes should be performed.

Back-up / Mitigation plan:

Security team will develop the best network architecture to eliminate risks defined. If breaches or compliance issues arise, anonymization and encryption techniques will be prioritized to ensure privacy, and regulator-approved adjustments will be made before go-live to safeguard personal and operational data.

A period in which the risk is relevant

Final stages and at the time of market release.

2. Regulatory Compliance Risks	High	Possible	Mitigating

Avoidance action:

With operations expanding multiple countries, the project can face challenges in complying with various local, national, and international regulations, especially concerning data protection (like GDPR). Legal experts are to be engaged early in the process to ensure full compliance with GDPR and other relevant privacy regulations. Regular audits of data handling processes should be performed.

Back-up / Mitigation plan:

Airport operation managers, harbour operation managers, TAV Tech Aviation academic consultants will guide the project team about the regulations. If incompatibilities occur, we will tailor deployments while retaining a common exploitation framework.

A period in which the risk is relevant

Final stages and at the time of market release.

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

Avoidance action:

The SINTRA platform involves integrating multiple technologies and systems. There's a risk that these systems may not integrate smoothly, leading to inefficiencies or failures. Modular architectures are to be planned and early cross-sector integration test across sites (airports, ports, etc.) are to be run.

Back-up / Mitigation plan:

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

A period in which the risk is relevant

Development and validation phases until project closure.

4. Commercial Adoption and Market Entry Risks	High	Likely	Monitoring & Controlling

Avoidance action:

A strong exploitation strategy with clear value propositions is to be built and early engagement with airports, ports, and municipalities is to be established. ROI through quantified KPIs should be demonstrated.

Back-up / Mitigation plan:

If market uptake lags, consortium will pivot towards niche verticals (e.g., construction site security, food safety monitoring) where entry barriers are lower.

A period in which the risk is relevant

End of project and first 2 years post-project.

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

Technological Evolution

During the first semester of 2025, we closely monitored several external technological and market developments that directly shaped the environment in which SINTRA operates. The most significant shift emerged from the European regulatory landscape, as the EU AI Act transitioned from a conceptual framework to phased obligations. In February 2025, the EU began enforcing bans on "unacceptable-risk" AI systems and introduced mandatory AI literacy rules. In August 2025, new requirements for general-purpose AI were added, with full enforcement planned for 2026. The European Commission confirmed there would be no delays, despite of the concerns from the industry. This means AI tools used in security and surveillance will face stricter rules soon.

Italy became the first EU country to pass a national AI law aligned with the EU AI Act in September 2025. The law includes criminal penalties for harmful misuse and clarifies rules around intellectual property. These changes make it harder for companies working across different countries to stay compliant

Cybersecurity developments also gained momentum. Although the NIS2 Directive became fully applicable across EU Member States in October 2024, its impact was seen in 2025 as national authorities began enforcing stricter compliance requirements. The scope now includes transport and port operators, demanding elevated security standards, greater accountability at the management level, and the risk of severe penalties for breaches.

Meanwhile, aviation and drone regulation continued to change. The European Union Aviation Safety Agency (EASA) refined its frameworks for beyond-visual-line-of-sight (BVLOS) operations and "Specific" category approvals, issuing updated SORA and eSORA methodologies. These incremental steps point to a steady progression toward scalable autonomous drone operations—directly relevant to SINTRA's UAV and UGV surveillance pilots.

Market and Industry Trends

Market dynamics changed as well. Surveillance technology providers especially Chinese brands such as Hikvision, faced growing restrictions, including outright bans in countries like Canada and increasing debate within the EU. This has driven airports, ports, and public authorities to prefer European and North American suppliers that emphasize secure-by-design and privacy-compliant technologies. At the same time, NIS2 obligations increased demand for integrated cyber-physical platforms that can prove regulatory compliance, changing buyer priorities. The market for AI-driven, multi-modal surveillance solutions is becoming more competitive, with both Horizon Europe projects and private companies targeting similar use cases in airports, ports, and industrial sites. Despite this, SINTRA's combined focus on multi-sensor fusion, federated and edge AI, and ethical governance remains unique and well aligned with these market pressures. In fact, the heightened demand for trustworthy AI and resilient critical infrastructure solutions has made SINTRA's approach more relevant than ever.

3. Market access & Exploitation

3.1. Partners' market access

Hoxhunt Oy	sme	FIN	16 PY
Hoxhunt works with large enterprise customers across the globe including key infrastructure companies across the globe. We are developing products aimed at reducing human risk for our clientele. More info on our partners program at: https://www.hoxhunt.com/partners			
TAV Technologies	ind	TUR	14 PY
As a start, TAV Technologies will make marketing presentations to the officials of TAV Group airports such as; Ankara Esenboga Airport, Izmir Adnan Menderes Airport, Gazipasa-Alanya Airport, Milas-Bodrum Airport, Antalya Airport, Tbilisi Airport, Batumi Airport, Enfidha-Hammamet Airport, Monastir, Habib Bourguiba Airport, Skopje International Airport, Ohrid St.Paul The Apostle Airport, Madinah Airport, Riga Airport, Zagreb Airport, Almaty Airport for both TAV Technologies own products to be developed during the project and for the products of SINTRA project partners. Initial sales activities will be executed in TAV Group Airports together with Alpata Technology and Kocsistem. After initial sales and system modifications according to the usage reports, solution will be presented to large (15M+ passengers), medium (2M - 15M passengers) and small (0M - 2M passengers) airports. TAV Technologies has identified Saudi Arabia, Qatar, Indonesia, India, and France as priority target countries with advanced marketing analysis, which is done by TAV Technologies R&D teams and published as an article with the name "ANALYZING THE SOCIAL FACTORS AFFECTING AVIATION DEVELOPMENT IN COUNTRIES BY CREATING A MIXED CURVILINEAR REGRESSION MODEL". The following strategies are planned to be implemented to reach targeted markets: • To present our new solutions to our existing customers in countries • Developing sales activities in target countries through business partnerships • Carrying out direct marketing and sales activities to potential airports in target countries • Increasing awareness and creating new business opportunities by organizing a digital marketing campaign in target countries			
University of Jyväskylä	uni	FIN	14 PY
For University of Jyväskylä, 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. The co-innovation enables fast feedback loop to early integration, which would not be available without it. University of Jyväskylä uses the 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 solutions. Both high-quality publications and experimental research work make the co-innovation together with companies more effective. In the SINTRA project, University of Jyväskylä strenghtens systematically its position as international-level research unit and light bearer in the technology domains that are significant to Finland.			
Bosch Security Systems B.V.	ifc	NLD	10 PY
The global market of IP-cameras for security and surveillance of critical infrastructure (without China) is estimated at almost 1.2 USD billions in 2021 and with a 10% forecasted growth per year will reach 1.7 USD billion in 2025. Within this segment, IP cameras with embedded deep-learning analytics are forecasted to grow by an average of 21% per year in the coming 4 years [OMDIA Video Surveillance and Analytics_World Database_July 2022]. The market leaders in the global video security market are Hikvision (China), Dahua Technology (China), Axis Communications (Sweden), Bosch Security and Safety Systems (Germany), Hanwha Techwin (South Korea), and Avigilon, a Motorola Solutions Company (Canada); and Bosch has around 9% share of this market, being a top-2 European leader. Bosch works closely with a big world-wide network of distributors and system integrators that can access the market of critical infrastructure surveillance. Over the past five years, we have had more than 1000			

projects in critical infrastructure surveillance, our tier-1 vertical, around the world, with more than 177 projects in airports including Antalya, Berlin Brandenburg and Dubai International airports, more than 168 projects in railways, more than 362 in government facilities, and more than 182 in industrial sites. Specifically in the Netherlands, Bosch is considered an important technology partner for surveillance of critical infrastructure, with large projects in Amsterdam Schiphol airport and Eindhoven city center. Bosch's goal within this project is to develop more intelligent and vertically adaptive solutions that will help to further strengthen its position in this highly competitive market of intelligent video surveillance systems. In R&D in Eindhoven, we focus on platform development for high end IP camera solutions, including multiple cameras and additional sensors to provide a better situational awareness. The unified physical security platform developed in the SINTRA project, which connects several sensing modalities, including video analytics, radar, multi-spectral sensors, is crucial for surveillance of critical infrastructure, maximizing the detection coverage and robustness, creating the data redundancy required for a layered detection approach during day and night and in different kind of weather conditions, and improving situational awareness and operational efficiency with a better incident understanding, threat verification and incident response. The development and deployment of such platform will further strengthen Bosch's position in the highly competitive market of intelligent video surveillance systems by providing not only the hardware (video cameras and recording systems) but also fully integrated surveillance solutions including video analytics. Bosch wants to focus on high end innovative solutions that could bring differentiation and help to keep our European leadership positions and to capture on average an additional 2% of global revenue per year in critical infrastructure protection, in the five years after the project.			
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".			
Koçtaş Yapı Marketleri Tic. A.ş	ifc	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.			
ViNotion BV	sme	NLD	9 PY
The company already delivers products and services for crowd analysis and traffic analysis with intelligent video camera systems since 2014. These products are being applied for the following applications: City marketing, retail footfall measurements, crowd management at events, and measurements of mobility to optimize public road infrastructure. ViNotion is on the market for more than four years with this product and gains market share. The end user for these applications are often public authorities and with this market access, we are increasingly active in the smart city and public safety sector. There is a strong desire to further optimized the video surveillance to support security operators and increase the efficiency. Tradditional surveillance is still human intense. Surveillance vehicles continuously patrol industrial area's and remote camera surveillance with human interpretation is very useful for reactive response and verification but hardly effective for proactive prevention. Using drones it is possible to cover larger areas, enable trigger-based surveillance and allow the security operations to have eyes at any location on demand. Our current network of drone operations and system integrators will allow us to enter the market swiftly.			
Avular Innovations B.V.	sme	NLD	7 PY
Avular is a for profit company with a yearly turnover of 2-3 million Euro. Avular has standing commercial contracts and relationships in a variety of different application domains and sectors, most prominently: industrial & infrastructural inspection, agriculture & horticulture & landscaping, construction & infrastructure. Avular does business in various EU member states and increasingly also outside the EU. Avular mostly operates as a system integrator or Tier 1 supplier as the mobile robot platforms need to be			

customized to fit a particular market need and the autonomy kit needs to be integrated in an existing piece of machinery. Commercial impact for Avular through the participation in the Sintra project is foreseen on two levels: -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. -indirect commercialization: Avular foresees that the Sintra project will lead to innovations that will lead to various new enabling technologies and new technical capabilities that can be incorporated in the core mobile robot platforms of Avular. This means that these new capabilities may spillover to applications in other sectors as well. These spillovers improve the competitiveness of the products of Avular and will thus give a boost to sales in various of our existing markets.			
MantiSpectra	sme	NLD	7 PY
MantiSpectra is commercialising unique near-infrared (NIR) sensors that can classify and quantify material composition using NIR light. Their ChipSense™ technology is the smallest fully-integrated NIR sensor on the market with a footprint of ~8 mm squared, ultra-low power consumption, and suited for volume production. The sensor can be integrated directly into the production line to monitor and control processes to increase efficiency and reduce waste, along the whole production and logistics chain for quality control of materials and assurance of 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 drug and explosive material identification. MantiSpectra expects to benefit in multiple ways from the outcomes of the SINTRA project: • A new product will be developed as a result of this project – a new compact, wireless sensor module suitable for on-site and in-field measurements. • Wireless data connection will be developed and tested, adding new capabilities to the sensor modules. • The sensor module would be evaluated in the application area of security via the measurement calibration process and development of machine learning models for illicit substances' identification. This process will open opportunities for market access related to e.g., drug and toxic substances' detection. • The TRL level of the sensor module will be increased following the on-field validation studies with end users in this project. • The integration of the sensor into a wider A.I. ecosystem will enable the sensors to bring impact and create value for a wide group of end users. • We expect that the innovations from this project will be relevant and lead to various new technical capabilities of the sensors, which can be incorporated into other application fields, e.g., in the manufacturing and agri-food industry. • Overall, we expect an increase in sales due to the adoption of our solution in new markets and the expansion of our reach.			
Second Nature Security Oy	sme	FIN	8 PY
After the project, 2NS will have deep knowledge, how to utilize AI and how to defend against AI related threats. Based on that information and knowledge, 2NS can create and commercialize services to help customers to utilize AI and also defend against AI based threat actors. As AI will play significant role in future, this will give huge commercial opportunities for 2NS.			
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. 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.			
Sorama B.V.	sme	NLD	7 PY
Sorama's go-to market strategy are utilizing its own sales force and business development, a Value Added Reseller (VAR) partner model and cooperation with strategic partners (e.g. Bosch, TU/e). For the harbor use-case that Sorama will be contributing in the SINTRA project, it is relevant to Sorama's current main markets, i.e. smart city, smart mobility, smart stadiums, and environmental monitoring. On one hand, technologies achieved within the harbor's safety and security use case are readily transferable to the smart city and stadiums applications – the common denominators of all these are on how to identify security threats based on sound information. On the other hand, installation of Sorama sensors will add further values to the harbor authorities who are interested in noise monitoring and compliance of vessels (based on Sorama's own market research). These benefits are all built upon the scalable Sorama Listener's platform and the harbor use-case realised in SINTRA will also act as a springboard for other harbors in Europe and in North America. Overall, being involved in SINTRA will further improve Sorama products, specifically in audio AI inference, data fusion with other sensors, sound localization, and software efficiency as well as stability.			
inosens	sme	TUR	6 PY
INOSENS is one of an AI based data analytics solution provider in Turkey and has good access to industry partners through the technology zone where INOSENS office is available. INOSENS will extend its market in AI based sensing technologies like mmWaveRadar for heatmap or other security scenarios and explainable capability of AI based systems by using AR as well as improving available solutions. 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. The project will allow INOSENS to validate the service and promote it to industrial applications. INOSENS will develop and promote dissemination material such as a demonstration for showcasing and white papers etc. as well as participating in industry events to promote the new developed product. The following strategies are planned to be implemented to reach targeted markets: • To present our new solutions to our existing customers in targeted countries • Make a sales plan activities in target countries through business partnerships • Increasing awareness and creating new business opportunities by using social media			
Jyväskylän ammattikorkeakoulu	uni	FIN	6 PY
One of Jyväskylä University of Applied Sciences' (Jamk) basic missions is to carry out research and development work that serves the business community in its region. Jamk has been at the forefront of developing Finland's national cyber security and resilience for more than ten years. In practice, this takes the form of cybersecurity-related research and development work in cooperation with companies in various sectors. Our partners include SMEs, large companies and also public actors, as in this project. In addition to research, development and innovation, we provide cybersecurity and data analytics training, testing and development services using the advanced Realistic Global Cyber Environment (RGCE) and its associated data analytics 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.			

Most of the end clients are public authorities like municipalities, police, large infrastructure (railway). Public authorities work by tenders. This is however the last phase. The first phase is market creation. Show that there is a product that can solve a problem. Then the public authorities will do a market consultation. Possibly some prove of concept projects. Then finally they write the tender. The company that created the market of course has a clear advantage. The after-market maintenance is also very important and is an evalutation criterium in most tenders. Macq alone cannot do this on a world wide scale. Cultural difference are also important to enter the market. Therefore we are building an international partner network. We have created sales material to help our partners. To help them create quotations for the tenders a shop has been set up. For an almost 100 year old company we are reinventing ourselves. Traditionally we always excelled in technology. Sales and Marketing have become mature and will take the next step. Our core business based on a modular approach is built to meet up with the most demanding end clients in Europe. To ensure the highest level of expertise and service level, we surround ourselves with exceptionally trustworthy local partners that also can guarantee after sales. We destinguish two different kind of critical infrastruture: large area and points. The first are harbours and airports. An example of the second are railway crossings. In Flanders there are 314 'black' dangerous road crossings. In 2018 there where about 20.000 accidents at road crossings with 16.000 harmed people, mostly cyclists. In Belgium there are1.713 railway crossings. In the Netherlands 1.900. In France 15.405. So already in our neighbouring countries there are a lot of market opportunities for new innovative traffic and mobility solutions to monitor the infrastructure but also protect the traffic participants.			
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 in internet enabled technologies. Our software has been integrated in varying applications in the public space, ranging from automated security monitoring to general quality of life improvements and logistic systems. Having previously partnered with high profile partners in the quadruple helix we are in a position fit for further growth in this market, with a strong desire to improve our product's maturity towards the stability levels required in large-scale deployments. Our software is a vital central component in eliminating human factors and interference as interoperability with more hardware inherently increases the options authorities have with gathered smart data. 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.			
Sensolus	sme	BEL	6 PY
Provide low-cost, easy to install and secure asset tracking solutions for construction yards. The solution will not only be sold the construction companies, but also in other segments like aerospace industrial manufacturing and transport and logics.			
SkyeBase	sme	BEL	5 PY
SkyeBase offers their total solution to industrial customers in the petrochemical and maritime sectors (e.g., container terminals, tank terminals, refineries, etc.). This total solution consists of (i) industrial robotic inspections via a Drones-as-a-Service license model and (ii) the I-Spect SaaS platform with AI defect detection and defect localization using digital twins. With this total solution, SkyeBase has already established a solid customer base in the BENELUX, enabling safe and cost-effective inspections and reporting of anomalies on critical infrastructure like STS container cranes, piping systems, and tank installations. Beyond these key focus areas, SkyeBase has also delivered solutions in industries such as			

construction, energy, and (public) infrastructure. SkyeBase has built a strong partner network with other robotic inspection companies in Belgium and abroad to scale its Drones-as-a-Service solution. It has also established multiple partnership agreements with notified bodies for statutory inspections of critical infrastructure in the petrochemical and maritime industries. Thanks to the ISO9001 and VCA petrochemical accreditation, SkyeBase holds a strong competitive position in these industries. Furthermore, through a strategic investment from Vinçotte Kiwa, SkyeBase now has even better market access, leveraging their extensive network and industry expertise to accelerate growth and expand its customer base. SkyeBase has recently obtained the European Light UAS Operator Certificate (LUC), enabling the company to scale up its industrial drone services across Europe by building operational privileges under this certification. The ultimate goal is to reach a point where SkyeBase can conduct any type of drone operation (VLOS/BVLOS) in the specific category without requiring separate operational authorization from the National Aviation Authority. SkyeBase aims to expand its total solution internationally by (i) creating additional value through the development of a new I-Spect industrial yard surveillance module, (ii) scaling to international markets through existing multinational customers, and (iii) leveraging its strong partner network to resell the total solution.			
Teleste	sme	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. Project results shall reinforce Teleste's future offering and competence and thus increase turnover in the public safety domain. 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.			
C-SITE	sme	BEL	4 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. We started our activity in Belgium, and to this day, approximately 2⁄3 of our revenue is generated from local construction projects. In the last two years however, we have expanded abroad. Yet this expansion would be in its early stages and mainly consists of projects where we 'follow' a Belgian company developing a project abroad. Although, we are also working directly with an increasing number of foreign companies. Currently, we are operational in construction sites across 8 countries: Belgium, Netherlands, Luxembourg, France, Germany, Ireland, United Kingdom and Slovakia. With more countries to follow such as Spain, Portugal, Poland, etc... Moreover, in June 2021, we also started our first project outside of Europe, in which we are monitoring the construction of the highest tower in Abidjan, Ivory Coast. In addition, we will			

proactively target the aforementioned countries to develop local contacts and leads. We have already started such sales and market penetration endeavours in the provinces of the Netherlands.			
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. 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. We believe that offering such an end-to-end solution will give us more leverage when talking to potential new customers and will give us a major advantage compared to competitors.			
KoçSistem Information Communications Services	ifc	TUR	4 PY
The technological advancements and challenges (defined in SoTA) open up several exploitation prospects in the market, particularly in industries that leverage object detection, human action recognition (HAR), and localization. Here are some key market access prospects: Surveillance systems benefit significantly from these technologies. HAR can identify abnormal behaviors (e.g., fights, illegal activities) in real time, while object detection helps in monitoring and tracking objects or individuals. This is applicable in public safety, security, and crowd management, where detecting specific threats or monitoring behaviors can improve response times and overall security.			
Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş.	sme	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.			
SIRRIS	res	BEL	4 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.			
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) with the knowledge of safety and security. Sintra will support SafeCity as an innovation advisor and will certainly give more work for the coming years.			
Secapp Oy	sme	FIN	3 PY
The role of the sensors and IoT in general is increasing when organizations are improving their preparedness and managing their unexpected situations such as emergencies and crises. Secapp is planning to utilize the projects results all SaaS platforms it is currently providing (i.e. in Finland, in the Middle East			

and in the North Africa) and for the customer segments and customers that are currently sing Secapp SaaS in these above mentioned platforms, taking into consideration customer segment and individual customer specific needs and requirements for data collection, exchange, use and storing. Also, the planned integrations for demonstrators in Port of Kemi will provide valuable showcase to further discuss with both existing and prospective customers.			
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.			
Airobot	sme	BEL	1 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). 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.			
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. Next year we will test this workarounds and then we will provide other harbour-areas with our workflows and anomaly-based scenario's. In semester 2 2024 we made the first step in this.			

3.2. Top 8 cumulative project achievements

1	Exploitation	New system	SINTRA multi-sensor Fieldlab #1 is installed at Port of Moerdijk	1
Summary		A fieldlab with 12 multi-modal sensors (acoustic, thermal and visual) and powerful GPU servel is installed at the Port of Moerdijk. The real-time communication lines sensors-server-public networks is set up. The sensors are synchronized with NTP server. This system is going to be used for data collection, AI training, testing, validation and further dissemination and exploitation of the project results.		
Impact		The first large multi-modal system set at industrial premises in EU. Impact: unique data from multi-modal sensors is recorded - gives the opportunity to learn and detect complex criminal behaviour. (quantification: NA)		
Partners		Eindhoven University of Technology, MantiSpectra, Avular Innovations B.V., ViNotion BV, Omines Internetbureau B.V., Bosch Security Systems B.V., Sorama B.V., SafeCity B.V., Port of Moerdijk		

2	Exploitation	New product	Measurement tool cyber risks of sensors	1
Summary		SafeCity has taken on the challenge of measuring cyber risks from sensors. The rapid development and implementation of sensor technology in critical infrastructure, such as logistics hubs and ports, have opened up new opportunities to enhance security, efficiency, and operational control. However, with these advancements comes the pressing challenge of ensuring the cybersecurity of these systems. The methodology to setup a measurement tool included literature reviews, risk analyses, interviews with experts, and an inventory of sensors and their applications. The instrument is a checklist		
Impact		A cyber risk measurement tool (checklist) with 100 questions divided in 5 components. With this checklist end-users can check the sensors before they buy these. (quantification: 8)		
Partners		SafeCity B.V.		

3	Exploitation	New system	Integrated camera gimbal	1
Summary		A COTS gimbal was integrated with a Nvidia Jetson platform for real-time video analysis and sensor fusion.		
Impact		The prototype will give us new opportunities for more leads in the drone market (quantification: 5)		
Partners		Eindhoven University of Technology, Avular Innovations B.V., ViNotion BV		

4	Exploitation	New product	CAM5 Railway crossing violation detection	1
Summary		The CAM5 Railway Crossing solution is designed to ensure the safety and fluidity of traffic at intersections where roads cross railway tracks. Using image analysis technology, this system not only detects vehicles violating railway crossing rules but also monitors these crossings to ensure that no vehicle is obstructing the railway. This dual-function approach not only facilitates the generation of infraction reports with visual evidence for enforcement and safety but also improves in the smooth operation of train traffic. The event-to-action framework allows for easy extensions.		
Impact		Railway crossing incidents and near accidents happen on a daily basis. Our new product is in the homologation process in multiple countries. There are about 105.000 railway crossings in the EU (quantification: 9)		
Partners		Macq		

5	Dissemination	Internal	Comprehensive literature review and detailed SOTA analysis	1
Summary		The integration of multi-modal sensing technologies and AI-powered data analysis has revolutionized the field of infrastructure security and safety. By combining data from various sensor modalities and existing data sources, a comprehensive and nuanced understanding of security and safety situations can be achieved. This approach enhances the detection of anomalies, maps them to potential threats, and facilitates coordinated responses. This literature study explores state-of-the-art technologies and methodologies in this domain.		
Impact		Comprehensive report (quantification: 5)		
Partners		Eindhoven University of Technology, MantiSpectra, TAV Technologies, Koçtaş Yapı Marketleri Tic. A.ş, inosens, University of Jyväskylä, ARD GROUP, Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş., SIRRIS, Macq, Avular Innovations B.V., KoçSistem Information Communications Services, ViNotion BV, Teleste, Omines Internetbureau B.V., Bosch Security Systems B.V., Sorama B.V., Airobot, C-SITE, SkyeBase, Secapp Oy, Second Nature Security Oy, Sensoan Oy, Jyväskylän ammattikorkeakoulu, Abloy Oy, Hoxhunt Oy, Port authority, SafeCity B.V., Port of Moerdijk, Citymesh, Sensolus		

6	Exploitation	New product	Development of new version1 small-footprint handheld sensor module	1
Summary		* The new, smaller electronic readout board for the NIR spectral sensor has been developed and fabricated. Stability tests are being finalized. * The first version of the module's outer chassiss has also been designed and fabricated.		
Impact		After further development and finalization of the full module system, the new sensor will be applied to the use case of measuring drugs. (quantification: 9)		
Partners		MantiSpectra		

7	Dissemination	Publication	Website	1
Summary		1. Setting up the website www.sintra-ai.nl 2. Getting the website name sintra-ai.eu and supporting to make it visible		
Impact		To gain attention, we need to have a website and show progress. (quantification: 4)		
Partners		Eindhoven University of Technology, TAV Technologies, SafeCity B.V.		

8	Exploitation	Enhancement	SINTRA PLATFORM GDPR DATA MAPPING	1
Summary		To assess GDPR compliance for the SINTRA platform, we created a GDPR data mapping requirement that identifies how personal data will be collected, processed, stored, and shared across the different platform features.		
Impact		The SINTRA platform will be able to ensure that all data processing activities are legally justified and that users are adequately informed. Up to €20 million Articles 83(4)-(6) Reduced Legal Costs (quantification: 20000000)		
Partners		Eindhoven University of Technology, TAV Technologies, University of Jyväskylä, SIRRIS, KoçSistem Information Communications Services		

3.3. Realised achievements

Dissemination	Exploitation	Standardisation	New company	Patent	Human capital
Total: 20	Total: 20	Total: 0	Total: 0	Total: 0	Total: 4

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. Deployment of GDPR-Compliant SINTRA Infrastructure at Airports

TAV Technologies completed the integration of SINTRA's core infrastructure with airport operational systems, linking camera feeds and real-time data collection under GDPR/KVKK compliance. This enabled pilot anomaly detection scenarios to run in a live operational context, validating not only technical robustness but also compliance with legal frameworks. This achievement ensures scalability and trustworthiness for future exploitation in sensitive environments.

2. Real-Time Anomaly Detection on UAV Platforms

ViNotion and Avular delivered a containerized object detection solution running directly on UAV compute units, capable of monitoring areas up to 5,000 m². This real-time capability represents a breakthrough for large-area surveillance, particularly in ports and open-air facilities. By combining RGB and thermal imaging, the system demonstrated robust performance under day and night conditions, significantly advancing autonomous aerial surveillance.

3. Development of Secure Data Sharing and Tamper Detection Mechanisms

Sirris and Sensolus advanced fragile watermarking and lightweight cryptography methods, ensuring data authenticity and secure sensor communication. These mechanisms were tested within BLE scanner networks and validated against real-world data collected in pilot sites. This step moves beyond conventional encrypted channels by embedding tamper detection into the sensor layer itself, providing trustable data streams for anomaly detection models and governance requirements.

4. Establishment of the Port of Moerdijk Field Lab with Multi-Scenario Pilots

The Port Authority, together with Bosch, Sorama, and TU/e, operationalized the Port of Moerdijk as a field lab, deploying over 40 cameras and conducting live scenario testing in two pilot zones (Appelzak and Plaza parking). These sessions included replaying anomalies to train AI models and refine detection scenarios. The achievement transformed the port into a living laboratory, providing large-scale, heterogeneous datasets essential for cross-modal AI fusion.

4.1.2. Top 4 next technical targets

1. Advanced Multi-Modal Sensor Fusion Algorithms

The consortium will focus on maturing fusion methods across RGB, thermal, acoustic, and multispectral modalities to improve robustness against complex anomalies such as smuggling or cargo theft. This includes refining unbiased detection techniques, cross-sensor alignment, and optimizing processing pipelines for edge deployment. Achieving this target will enable higher detection accuracy under variable lighting, weather, and crowd-density conditions, moving SINTRA closer to operational-grade anomaly detection.

2. Expansion of UAV/UGV Autonomous Surveillance Pilots

Building on successful UAV trials, the next period will extend to coordinated UAV and UGV deployments with semi-autonomous flight and driving patterns. Partners will test BVLOS-compliant operations under the LUC framework and validate real-time onboard AI detection during joint scenarios at port and construction sites. This target aims to prove multi-agent collaboration and establish SINTRA as a pioneer in integrated autonomous surveillance fleets.

3. Federated AI and Privacy-Preserving Learning

The project will deploy and validate federated learning frameworks across multiple pilot sites (airports, ports, retail). Models will be trained on local nodes without raw data transfer, incorporating homomorphic encryption and lightweight cryptography to ensure GDPR/KVKK compliance. The goal is to demonstrate that accurate AI models can be developed across distributed environments, reducing latency and enhancing trust in real-world deployments of critical infrastructure security systems.

4. Full Demonstration of Port and Airport Field Labs

During the next reporting period, SINTRA will scale pilot activities, including more scenarios at the Port of Moerdijk and extended airport trials. Planned activities include replaying and recording complex threat events, refining anomaly detection models with real-world datasets, and validating dashboard usability. This target ensures that SINTRA's solutions move from prototype to demonstrator level, providing evidence of scalability, interoperability, and readiness for exploitation.

4.1.3. Top 4 issues

1. Delay in Field Lab Setup and Data Availability

Details:

Delays in completing installations at pilot sites, particularly the Port of Moerdijk, slowed down real-time data availability and postponed some software validation activities.

Impact:

Moderate delay in testing and validation phases, causing rescheduling of integration work.

Mitigation action:

Partners used simulated datasets and smaller-scale testbeds to maintain algorithm development. Remaining impact exists but expected to be cleared in next semester with full site readiness.

2. Hardware and Sensor Integration Challenges

Details:

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

Impact:

Reduced scope of anomaly detection validation during 2025-1. Incompatibility between systems deteriorates real-time data processing and decision-making, causing inefficiencies in AI-driven automation and increasing project complexity and resource demands.

Mitigation action:

Modular integration strategy and middleware solutions introduced; staggered validation is underway. Residual issues remain but are being systematically reduced with partner-specific test setups.

3. Regulatory and Compliance Delays for UAV Operations

Details:

Obtaining approvals for UAV and UGV pilot operations under BVLOS conditions took longer than anticipated, especially due to evolving national requirements.

Impact:

Postponement of some autonomous flight scenarios, limiting early validation opportunities.

Mitigation action:

Focus shifted to simulation and local VLOS flights while BVLOS applications proceed. Remaining impact is temporary; approvals are expected in 2025-2.

4. Resource Allocation Variances Across Partners

Details:

Some partners (e.g., smaller SMEs) underperformed against planned efforts due to financial or organizational constraints, affecting progress in specific WPs.

Impact:

Gaps in workload distribution and slower progress in cross-consortium deliverables.

Mitigation action:

Larger partners absorbed critical tasks; workload redistribution agreed. Some residual impact persists, but corrective planning ensures balanced contributions in forthcoming period.

4.1.4. Status of deliverables

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

The total number of deliverables in the project is 30.

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

From the start of the project until the end of this reporting period, 17 deliverables are supposed to be finalised. These are:

- D1.1 Use case analysis and stakeholder requirements,
- D1.2 Hardware architecture and communication specifications,
- D1.3 Sensor and data source inventory report,
- D1.4 Privacy and data governance analysis report,
- D1.5 Use case specific sensor and data source integrations,
- D1.6 Platform architecture design document,
- D2.2 Ethical data handling guidelines report
- D2.3 Cybersecurity measures implementation report
- D4.1 Data governance protocol,
- D4.2 Data management plan,
- D5.1 Public/internal website,
- D5.2 Dissemination and communication plan,
- D5.3 State-of-the-Art analysis,
- D5.4 Current and perspective business models
- D5.5 Exploitation plan
- D6.1 Project and risk management plan,
- D6.2 Progress and quality assurance report 1 (M12).

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

From the start of the project until the end of this reporting period, 17 deliverables have already been finalised. These are:

- D1.1 Use case analysis and stakeholder requirements,
- D1.2 Hardware architecture and communication specifications,
- D1.3 Sensor and data source inventory report,
- D1.4 Privacy and data governance analysis report,
- D1.5 Use case specific sensor and data source integrations,
- D1.6 Platform architecture design document,
- D2.2 Ethical data handling guidelines report
- D2.3 Cybersecurity measures implementation report
- D4.1 Data governance protocol,
- D4.2 Data management plan,
- D5.1 Public/internal website,
- D5.2 Dissemination and communication plan,
- D5.3 State-of-the-Art analysis,
- D5.4 Current and perspective business models
- D5.5 Exploitation plan
- D6.1 Project and risk management plan,
- D6.2 Progress and quality assurance report 1 (M12).

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

No, there are not any deliverables delayed.

4.1.5. Statement on project progress during the reporting period

As of the first half of 2025, SINTRA is progressing in line with its objectives, with field labs operational at key sites including the Port of Moerdijk and airports, and initial pilots demonstrating multi-modal anomaly detection and GDPR-compliant data collection. The consortium has delivered significant advances in UAV-based detection, edge AI integration, and secure data sharing. While overall progress is strong, some delays occurred in hardware integration and data availability, mainly due to extended field lab setup and regulatory clearances for drone and sensor deployments. These were mitigated through simulation environments and phased validation, keeping the project on track.

4.2. Details of progress per Work Package

WP 1: Use cases, requirements & architectural specification

WP1 was scheduled to end in M12. There are however deliverables that need improvement or updating.

There are ongoing discussions on the platform architecture.
"D1.6 Stakeholders' platforms and architectures designs document" will be updated once the growing consensus has matured.
In the meantime work on the platform has started. The results will be reported in the WP2 deliverable "D2.6 Platform design report" which is due M30.
The platform team has monthly meetings.
The platform will be a concrete design also proposed in the FPP. We are in the process of describing an architecture based on open source components that can be aligned in different configurations. This will be complemented by a more abstract model on how instances of this platform can work together.

An update of the combined deliverable "D2.2 Hardware architectures and communication specification document" and "D2.5 Use case specific sensor and data source integration plan" is almost finalised.

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

WP2 advanced the SINTRA platform architecture, delivering specifications for edge and federated AI deployments. Ethical data handling guidelines and cybersecurity implementation reports were finalized. The consortium defined modular integration pathways for multi-sensor data, ensuring interoperability across airports, ports, and construction sites. Completion of D2.2 and D2.3 marked a key step, providing the governance backbone for privacy-preserving AI.

The D2.2 Ethical Data Guidelines Report: This report defines the ethical, legal, and technical framework guiding the SINTRA platform, ensuring compliance with GDPR and anticipating the EU AI Act. It emphasizes privacy-by-design, transparency, fairness, accountability, and safety in AI-driven,

multi-modal surveillance across airports, ports, construction sites, retail, and mobile environments. The SINTRA architecture is structured into four layers: secure data ingestion (Message Broker), AI logic and sensor fusion (Business Definition), aggregation and APIs, and visualization dashboards with AR interfaces. Ethical foundations include minimizing data collection, enforcing purpose limitation, ensuring human oversight, and conducting fairness audits to prevent bias. A six-stage data lifecycle governs collection, processing, storage, analysis, retention, and deletion, supported by clear controller/processor roles, joint controller agreements, immutable audit logs, and cross-border safeguards (SCCs, TIAs, BCRs). Privacy-enhancing technologies—federated learning, differential privacy, homomorphic encryption, and secure multi-party computation—are embedded to protect identities while enabling advanced analytics. Overall, the report delivers a blueprint for deploying SINTRA responsibly, balancing operational effectiveness with fundamental rights and societal trust.

The D2.3 Cybersecurity Measures Implementation Report: This report addresses the risks and protective strategies for sensor-based systems in critical infrastructure such as airports, ports, and industrial sites. It identifies four main attacker types—nation-state actors, hacktivists, cybercriminal groups, and insiders—highlighting their motivations from espionage and sabotage to financial extortion. The report details the impact of cyberattacks on aviation and maritime sectors, ranging from manipulated air traffic control data and compromised biometric access systems to disrupted cargo logistics and spoofed vessel navigation. Real-world cases such as the NotPetya attack on Maersk and ransomware at Nagoya Port illustrate both financial and operational consequences. It highlights the diversity of sensors (radar, LiDAR, biometric, chemical, magnetic, imaging, etc.) and their unique vulnerabilities, including insecure firmware, weak authentication, and supply chain risks. Common threats include DDoS, ransomware, spoofing, and malicious firmware injection. Risk management frameworks—NIST CSF, ISO/IEC 27005, OWASP IoT, and ISA/IEC 62443—are assessed for applicability, stressing a shift from IT's confidentiality focus to OT's safety and availability priorities. The report concludes with a practical checklist of ~100 questions for end-users to evaluate sensor security across hardware, software, data handling, supplier integrity, and user responsibility, promoting lifecycle-based, context-specific cybersecurity.

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

During the reporting period, substantial progress was achieved in the development and testing of advanced anomaly detection systems across multiple sectors, including airports, ports, construction sites, retail, and food and beverage environments. Alpata led efforts in anomaly detection by utilizing video, thermal, and acoustic data. Inosens contributed by leveraging radar-based 4D point cloud data to identify anomalies, laying the groundwork for detecting unauthorized access and unusual situations in security-critical areas. Vinotion implemented a containerized real-time object detector for drone-based people detection and explored sensor fusion methods that combine RGB and thermal imaging. SkyeBase made advancements in researching and testing state-of-the-art multi-modal AI models for anomaly and threat detection, validating initial prototypes through field tests. TU/e developed a multi-modal video anomaly detection prototype that generates sensor modalities from RGB streams. Their work also included the implementation of a mixture-of-experts system and techniques for spatial localization of anomalies within video footage. Sirris developed drone-based methods for detecting and tracking suspicious individuals, as well as static camera-based techniques

for identifying suspicious scenes using behavioral and contextual features. Koçtaş addressed loss and smuggling scenarios through multimodal analysis of camera footage and cash register logs. They employed the YOLOv8n-Pose model for human and product detection and used the DeepSORT algorithm to track people and products over time. Kocsistem adapted AI models, created new training and evaluation metrics, and conducted research on anomaly localization methods.

Field testing and prototyping played a central role in many partners' contributions. Several field tests have been set up where the different partners have collaborated for the pilot scenarios definition, simulate scenarios, data collection. Avular built and tested its first prototype of the Vertex UAV, integrating ViNotion's software in a field lab for port use cases. SkyeBase validated its initial AI model prototypes through field tests focused on anomaly and threat detection. TAV established a new field lab and executed pilot scenarios that simulated real operational conditions, testing the system's ability to detect, record, and analyze events in near real-time. In the retail and food sectors, ARD focused on anomaly detection in food and beverage environments by preparing scenarios and recording field test videos.

Data collection and integration were key themes throughout the reporting period. Partners focused on dataset preparation, including anonymization, registration, and synchronization across modalities. Sirris developed methods for automatic alignment of RGB and thermal images and for anonymizing faces and license plates. Keenfinity enhanced the quality of thermal images under challenging conditions, contributing to the robustness of AI systems and supporting data collection during field tests at PoM. CityMesh worked on integrating unmanned ground vehicles (UGVs) and unmanned aerial vehicles (UAVs) into a local subsystem to facilitate data collection for further training. C-Site participated in two large-scale data collection campaigns, capturing and curating construction site footage and organizing the video data to support training, benchmarking, and validation tasks. Hoxhunt advanced its SaaS Human Risk Reduction platform by integrating data from multiple sources to create a comprehensive situational awareness picture. They also collaborated on data integration for a port use case in Finland. TAV implemented an automated data collection system based on a distributed microservices architecture, integrating PostgreSQL, Redis, and MinIO for efficient storage and processing. This platform enables scalable, continuous, and reliable video data capture and processing, significantly reducing manual workload and ensuring consistent datasets for evaluation. ARD contributed to data anonymization in videos, created datasets using open-source data, and processed air quality data (PM2.5, PM10) obtained from TAV.

WP 4: Cross-coordination, visualisation, and demonstrators

In WP4 deliverables D4.1 and D4.2 are finalized. The partners that are involved in the different use case fieldlabs are gathering and sharing data compliant with the protocols of D4.1. The data is being used by the partners to conduct the research and development of the AI technology. More specifically, per use case:

- UC1a Airport :

In the 2025/1 semester, cross-coordination frameworks were established to enable secure and GDPR-compliant sharing of multimodal data, including camera feeds and sensor outputs, among stakeholders. Within this scope, initial dashboards were built to visualize real-time event monitoring

and situational awareness in critical airport areas, laying the foundation for operational demonstrators. The automated video data collection and processing platform was successfully integrated into existing airport-like infrastructure, supporting AI-driven object detection, anomaly recognition, and event classification modules. Scenario-based pilot testing began, measuring system response times, accuracy, and processing performance, with early results guiding system optimizations. These efforts positioned the airport use case as a practical showcase of how AI and multimodal sensor integration can enhance safety and operational intelligence in high-traffic environments.

- UC1b Food & Beverage :

Parallel progress was achieved in the food and beverage retail use case led by Turkish companies. Here, cross-coordination centered on integrating IP camera streams with POS system data to detect theft or anomaly scenarios at checkout counters, supported by AI-based object recognition and event classification. Visualization prototypes were prepared to display customer movements, product handling, and anomaly alerts in real-time dashboards. Pilot scenarios, including loss prevention, sudden incidents in dining areas, and crowd monitoring, were tested with anonymized and GDPR-compliant datasets. Automatic data pipelines ensured that video and sensor data were captured, anonymized, and processed without manual intervention, enabling scalable demonstrations. These activities validated the adaptability of SINTRA technologies beyond airport environments, highlighting their effectiveness in retail and hospitality domains where safety, loss prevention, and customer well-being are equally critical.

- UC2 Maritime Port :

in Sept 2024 first sensor data was captured and recorded and a new session for recordings in Sept 2025 is being prepared at the Port of Moerdijk. Several scenarios such as hiding people in e.g. trucks, intrusion and smuggling, etc were played with actors. The data was anonymized in real-time, synchronized and stored on a secure server. For the sea port of Kemi, secure data collection and sharing mechanisms are researched and analyzed as part of T4.1. Collaboration with Bosch security started and Bosch sensor data sharing from the Kemi seaport use case initially planned, and mechanisms to guarantee privacy. As the Finnish partners started later, the activities for task T4.2 are just recently initiated. Collaboration with Port of Moerdijk and North Sea port has started and the Finnish partners visited the port of Moerdijk to synchronize the activities between all partners that are involved in UC2 Maritime port.

In Belgium the consortium partners had a meeting with DP World Antwerp to align on relevant scenarios including perimeter control, detection of fence damage and intrusion, surveillance of unsupervised locations at night, and correlation of alarms within the control room to support decision-making. In addition, a data collection day took place in Rumst focusing on the Tomorrowland containers, where data was collected from static cameras (Macq, C-Site), drone cameras (Skyebase, Citymesh), a robot-mounted camera (Citymesh), and BLE sensors (Sensolus). The local 5G network of Citymesh was used during the test. The involved partners (Macq, C-Site, Skyebase, Citymesh, Sensolus, Sirris) have applied this dataset to develop methods for RGB–infrared alignment, drone-based detection and tracking of suspicious individuals, and the analysis of suspicious scenes with static cameras using behavioural and contextual features. Pipelines for anonymising sensitive information such as faces and license plates and for real-time scene suspicion evaluation were developed, and the collected footage was used for model training and validation.

Parallel work has also continued on secure data sharing with zero-trust concepts and the protection of BLE communications with lightweight cryptography, ensuring that the solutions remain secure and compliant with GDPR and privacy protection requirements.
- UC4 Construction site:
A data collection day was organised in Malle on a hospital construction site, where data was collected from static cameras provided by Macq and C-Site, drone cameras operated by Citymesh, and BLE sensors supplied by Sensolus. The local 5G network provided by Citymesh was used during the test. Using this dataset, the partners (Macq, C-Site, Citymesh, Sensolus, Sirris) developed methods for automatically aligning RGB and infrared images based on maximization of mutual information, detecting and tracking suspicious persons with drones, and recognising suspicious scenes with static cameras through behavioural and contextual features such as fence climbing. In addition, pipelines were created for blurring faces and license plates (in line with GDPR) in drone images and for evaluating scene suspicion in real time. The collected footage has been used for training and validation of the above methods. Work has also continued on secure data sharing based on zero-trust approaches and on securing BLE communications with lightweight cryptography solutions.

The visualization part of Task 4.2 is under development, but since the integration of all AI subcomponents has not started, the visualisation work to effectively showcase the capabilities of the SINTRA platform, while also providing end-users with an easy-to-use interface for accessing and analyzing the data will continue.

WP 5: Dissemination & exploitation

Deliverables 5.4 and 5.5 are finalized.

Academic conference publications and talks on SINTRA innovations:
- Laurens Le Jeune, Anna Hristoskova, and Farhad Aghili, Fast and robust fragile watermarking enabling real-time self-recovery for UAS, Critical Infrastructure and Manufacturing System Security (CIMSS) at the conference on Applied Cryptography and Network Security (ACNS) in Munich on 23-26th June.
- Majhi, S., D'Amicantonio, G., Dantcheva, A., Kong, Q., Garattoni, L., Francesca, G., Bondarau, E. & Bremond, F., Just Dance with pi! A Poly-modal Inductor for Weakly-supervised Video Anomaly Detection. 13 Aug 2025, 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition, CVPR 2025. Institute of Electrical and Electronics Engineers, p. 24265-24274 10 p. 11092984
- Wang, Y., D'Amicantonio, G. & Bondarau, E., Near-incident detection in railroad environments: lateral distance estimation from train-mounted monocular camera. 15 Sept 2025, 2025 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, CVPRW 2025. Institute of Electrical and Electronics Engineers, p. 2027-2036 10 p. 11147850

SINTRA Presentations at Industrial conferences and Expos
- Presentation at ISCWest, Las Vegas, USA, March 31 - April 4, 2025,
- Presentation at Intersec, Dubai, UAE, January 14 - 16, 2025,

- eRIC (Disaster Management Expo),
- GENETEC conference 2025,
- NENOVA knowledge day 2025. The project was discussed, and its added value and interim results were discussed,
- Critical Communications World in Brussels on 17-19th of June 2025.

SINTRA exploitation discussion with end-users:
- Brabant Ports (all inland ports of the provicne of Brabant),
- BTT (Barge Terminal Tilburg),
- Port authority of Malaga,
- van Berkel Logistics (Terminal operator),
- SINTRA port use case presentation at DP World harbour,
- Exploitation with Rotterdam World Gateway,
- Deployment discussions with drone inspection companies Vincoitte, Kiwa (BE).

Prototypes and Pilots:
- SINTRA Fieldlab#1 is installed in Truck Parking area in Port of Moerdijk, Netherlands – acoustic, thermal and video sensors, 12 sensors in total. Computation server is installed at PoM and connected to the sensors for constant recording.
- Deployed prototype of activity monitoring in Malle construction site.
- Pilot of KocSistem's framework HOLMESVAD/Holmes-VAU in one of the airport of TAV Technologies.

WP 6: Project Management

WP6 maintained coordination through regular international and national meetings. During this reporting period, WP6 ensured consistent consortium coordination. Weekly international and national meetings were held, enabling effective alignment across partners. The first ITEA4 Progress Review was completed online with participation from all partners, and TÜBİTAK audits were successfully passed. Dissemination and communication strategies were updated, with internal collaboration tools (Google Drive platform) used for structured document sharing. Deliverables were on schedule: 17 out of 30 planned were finalized by this reporting period. Risk management was actively pursued, mitigating challenges in UAV regulatory approval and multi-sensor integration.

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
KoçSistem Information Communications Services	2.03	2.03	Aylin Yorulmaz
	Main contributions during the reporting period: Efforts focused on adapting and validating deep learning models (PEL4VAD, HOLMESVAD, HOLMES-VAU) for multi-class anomaly detection in videos. Model architectures, loss functions, and evaluation metrics were optimized; datasets were restructured and analyzed. Confidence scores, forced anomaly prompts, and NER-SAM integration were tested to enhance detection and localization performance.		
	Discrepancy explanation: no discrepancy		
Omines Internetbureau B.V.	2.84	1.50	Niels Keurentjes
	Main contributions during the reporting period: We have assisted the team with our knowledge and insights in large scale software applications, taking the technical lead in setting up and maintaining the network and software architecture of the field lab. We have participated in R&D discussions and prototyping regarding possible security and detection scenarios, and have commenced designing and wireframing dashboards and practical applications.		
	Discrepancy explanation: Delays in field lab setup have caused subsequent delays in the availability of software and data required for our tasks.		
ViNotion BV	5.26	5.42	Egbert G.T. Jaspers
	Main contributions during the reporting period: For T3.2, A containerized real-time implementation of an object-detector that can detect people on large areas up to 5000m2, was realized on an AI compute platform of the Avular drone. For T3.1, research is being performed on sensor fusion combining RGB and thermal imaging to enable detection at day and night. As a first step, image registration and alignment was designed and the research on unbiased object detection is progressing well. Scientific papers for publications are being prepared.		
	Discrepancy explanation: The progress is in line with the planned effort.		
Koçtaş Yapı Marketleri Tic. A.ş	4.47	4.00	Gizem Yeldan
	Main contributions during the reporting period: Developed a real-time loss prevention system integrating IP camera footage and POS logs to detect anomalies around checkout areas. Achieved successful human and product tracking using YOLOv8n-Pose and DeepSORT. Ensured GDPR/KVKK compliance with local-only data processing. Initiated anomaly detection model training based on human pose analysis for scenarios like unscanned product concealment.		
ARD GROUP	2.63	2.83	Arda Ödemiş
	Main contributions during the reporting period: During this period, ARD focused on data collection, preparation, and analysis while ensuring privacy and GDPR compliance. We created and then recorded scenario-based videos and anonymized all personal data		

	through face blurring. These videos supported tests on anomaly detection such as falls, fights, and sudden/fast running. In parallel, ARD explored external datasets, extracted feature maps for AI training, and started initial experiments on crowd detection and air quality analysis.		
Teleste	1.70	0.88	Jani Väre
	Main contributions during the reporting period: - Definition and implementation of Teleste SaSe platform. - Clarifying regulatory issues e.g regarding GDPR. - Joint work with other finnish project partners in tackling use cases and drafting PoC setups with other finnish partners.		
	Discrepancy explanation: Project start was delayed and hence the estimation of actual effort did not meet planned values.		
University of Jyväskylä	8.35	0.89	Markus Sihvonen
	Main contributions during the reporting period: We are delivered contribution to all WP1 deliverables. We did define Finnish use case with all Finnish partners. We did define initial architecture to the Kemi seaport data collection platform. Implementation of the starts after summer 2025.		
	Discrepancy explanation: We did started the project January 2025 and therefore have only worked in the project total of 6 months.		
Citymesh	2.09	2.17	Noa Lambert
	Main contributions during the reporting period: During the third semester of the project citymesh was mainly involved in the Belgian demo and data collection day. This day combined our effort of integrating our UGV and UAV together in our local subsystem in order to collect the necessary data for further training. This system can be further expanded upon to integrate in the cross-country data sharing.		
	Discrepancy explanation: We worked hard to prepare the demo/test day in April 2025, hence our effort is distributed more towards the first half of the year. We expect to match the planned effort by the end of the year.		
TAV Technologies	6.66	6.32	Talha Koc
	Main contributions during the reporting period: TAV Technologies has deployed the core SINTRA infrastructure, completing camera integrations and launching GDPR-compliant data collection and processing platforms. In this semester TAV has also succeeded in advanced AI integration with operational systems, conducted pilot scenario tests that support innovation in anomaly detection and align with business goals for secure, scalable airport operations.		
	Discrepancy explanation: No discrepancy		
SIRRIS	1.72	1.49	Farhad Aghili
	Main contributions during the reporting period: WP1: Supported BE consortium in defining the port security use case with DP World, extracting requirements and scenarios. WP2: Developed fragile watermarking for tamper detection and sensitive data recovery, with a related publication; secure data sharing with zero-trust concepts and the protection of BLE communications with lightweight cryptography. WP3: Created methods for RGB/IR alignment, suspicious person tracking, scene detection, anonymisation, and validated models with collected data.		

SafeCity B.V.	1.25	1.25	Jan Otten
	Main contributions during the reporting period: SafeCity attends the Dutch meetings weekly and also writes the minutes. International meetings are attended monthly. SafeCity is a member of the Sintra platform group. This semester, significant attention was paid to cyber risk measurement, and SafeCity wrote the vast majority of this deliverable 2.3. SafeCity facilitated the contacts for this, particularly with the Finnish partners. SafeCity is working with partner Omines to develop an online cybersecurity checklist for sensors.		
	Discrepancy explanation: no discrepancy		
inosens	3.16	1.53	Ismail Uzun
	Main contributions during the reporting period: We mostly spend time on AI model development and attended all technical and management meetings.		
	Discrepancy explanation: As INOSENS, we contributed all work packages and it is done as planned.		
MantiSpectra	3.70	3.70	Fang Ou
	Main contributions during the reporting period: Development and further testing of chip and new boards Contacts and discussions with national Police to measure illicit substances- delayed on request of police till 2025H2 Contributions to the Port of Moerdijk use-case and weekly Dutch national meetings		
Eindhoven University of Technology	4.38	4.15	Egor Bondarev
	Main contributions during the reporting period: 1. Four (4) research papers are published at international peer-reviewed conferences. 2. Second prototype of video-based detection of behaviour anomalies is developed. 3. A method for spatial localization of anomalies detected in videos is developed. 4. An international SINTRA workshop is organized in June 6, 2025, at Port of Moerdijk. 5. A GPU-based computation server is designed and installed at the Port of Moerdijk. 6. Several full-day dataset collection sessions are organized at PoM.		
	Discrepancy explanation: No discrepancy. We are running at full speed with 2 PhDs, post-doc and associate professor in the TUE SINTRA team.		
Necdet Alpata Pazarlama Lojistik ve Turizm Sanayi ve Ticaret A.Ş.	2.39	2.00	Murat Sağlam
	Main contributions during the reporting period: In the SINTRA project, Alpata developed AI-based anomaly detection models for processing data obtained from multiple sensors (camera, lidar, and environmental sensors). During this period, a hybrid training dataset was created by combining open-source datasets (kaggle, etc.) with scenarios provided by project partners. Alpata conducted initial model training on this dataset using deep learning-based behavioral analysis and multimodality fusion methods.		
	Discrepancy explanation: No discrepancy. We are running at full speed with our team.		

Bosch Security Systems B.V.	4.81	4.41	Ildiko Suveg
	Main contributions during the reporting period: We focused on enhancing image quality for thermal devices, including automatic contrast adjustment based on scene characteristics, as well as manual sharpening controls. These improvements are designed to boost image quality under challenging conditions, contributing to the robustness and reliability of the AI-based system. In collaboration with Sorama, TU/e, and Omines, a field lab was successfully installed at the Port of Moerdijk. This facility enables the collection of real-world data throug		
Abloy Oy	1.63	0.30	jesse.juurelma@abloy.com
	Main contributions during the reporting period: Preparing data for other partners to be processed, creating architectural plan with other partners.		
	Discrepancy explanation: After we discussed with our other Finnish partners we saw that we will be data provider for other partners, and because of that there hasn't been technical implementations done.		
Hoxhunt Oy	10.31	6.82	Pyry Åvist
	Main contributions during the reporting period: Research and development of the SaaS human risk analysis, mitigation and visualisation platform and related AI tools and components continued. In addition, collaboration plans have been made between Finnish partners related to the Port Use Case.		
	Discrepancy explanation: Finland joined the project at the end of 2024 so we are still catching up.		
Jyväskylän ammattikorkeakoulu	2.45	0.36	Aimo Pellinen
	Main contributions during the reporting period: Kick-off meeting, One-on-one meetings with Finnish companies in the project. Use case specification with the consortium, requirements & architectural specification with partners. Dissemination planning.		
	Discrepancy explanation: The project started for Finnish partners during this semester. Cooperation with other partners geared up to initial levels.		
Sensolus	3.54	3.93	laurence claeys
	Main contributions during the reporting period: The secure BLE solution with 128-bit encrypted tag-to-scanner protocol codeveloped with Sirris is advancing cloud implementation. Sensolus specified battery/wired BLE scanners with edge algorithms. Rigorous testing of 10 prototypes took place in the Sensolus office, Malle hospital campus, and Tomorrowland's 5-hectare Rumst storage site. In WP 3.2, Sensolus is investigating the possibility of anomaly detection via data fusion and AI-based breach detection using movement patterns.		
Sorama B.V.	3.67	4.79	Thomas Willems
	Main contributions during the reporting period: Sorama supported the installation of the Port of Moerdijk field lab and configured its acoustic sensors for integration and data collection. We participated measurements and contributed to data gathering for AI model training. Work continued on classification and anomaly detection algorithms for edge processing, and development started on a submersible acoustic sensor variant for maritime use.		
	Discrepancy explanation: Higher effort is due to additional R&D for a submersible acoustic sensor		

	variant, which was not part of the original scope, combined with extensive work on setting up and maintaining the Port of Moerdijk field lab, including integration and troubleshooting alongside planned anomaly detection tasks.		
Avular Innovations B.V.	3.82	3.71	Gino Van der Zijde
	Main contributions during the reporting period: We've created a first prototype solution of our Vertex UAV with integrated software from SINTRA partner ViNotion . Furthermore, a major achievement was the first test flight and data gathering flights with the Vertex UAV which have been performed above open fields, forests and above the Port of Moerdijk (Appelzak area).		
	Discrepancy explanation: The actual effort is in line with the planned effort.		
Secapp Oy	1.36	0.32	Timo Harju
	Main contributions during the reporting period: The project is progressing steadily with partners collaborating on a working plan. Planning sessions with the Port of Kemi shaped the scope and setup of demonstrators, while discussions clarified key user requirements. A visit to the Port of Moerdijk provided insights into local challenges. Meetings with partners outlined common initiatives and technical interfaces, ensuring alignment and interoperability across technical elements.		
	Discrepancy explanation: Funding decision arrived fairly late, postponing ramp up activities of the project. The national project kick-off was in mid-January, after the actual activities had an opportunity to start.		
Second Nature Security Oy	2.00	3.00	Juho Ranta
	Main contributions during the reporting period: Participation in Finnish use case (Kemi seaport), partner collaboration between the Finnish project partners, research collaboration with Finnish academic partners for AI driven threat defence and security testing, concept development for AI assisted security monitoring service including the external attack surface assessment features.		
	Discrepancy explanation: More effort has been used as there has been an optimal timing with regards to planned activities in the project and technological evolution of the AI assisted threat defence (e.g. with regards to AI assisted security monitoring) and also of the AI assisted security testing. This is resulted in increased effort, but rapid advancement in results.		
Sensoan Oy	1.25	0.02	Kari Petteri Malmivirta
	Main contributions during the reporting period: During the reporting period, Sensoan has actively participated in the regular international and local meetings of the SINTRA consortium. In addition, we have held discussions with several partner companies and universities. A brief technology assessment of DECT NR+ has also been conducted.		
	Discrepancy explanation: Our company, Sensoan, has not been able to carry out the original plan due to financial difficulties, which have also required temporary layoffs. At the moment, the company is undergoing an acquisition process that will result in organizational changes.		
SkyeBase	2.18	2.09	Tom Daniëls

	Main contributions during the reporting period: SkyeBase advanced the development of the yard surveillance module by integrating live video, drone data into a first prototype. We made the first progress by collecting relevant data at Tomorwland and re-training our AI models for context-aware anomaly detection & object tracking. Further actions have been taken together with sirris to improve platform security. Operationally, we prepared semi-autonomous surveillance flights under our LUC certification, supporting SINTRA's BVLOS ambition		
	Discrepancy explanation: No significant delay during the last reporting period. Actively working to compensate for the slower start of the project in the beginning.		
C-SITE	1.90	1.13	Jelle Stuyvaert
	Main contributions during the reporting period: During the first semester of 2025, C-SITE focused on extending its activity monitoring functionality and further developing the dashboard for visualization. In parallel, additional data collection was carried out on construction sites in collaboration with Belgian partners, providing input for future AI-based analytics.		
	Discrepancy explanation: The discrepancy (planned 1.90 PY vs. actual 1.13 PY) is due to C-SITE's approved (by VLAIO) change request reducing its contribution from 100% to +-10% of the original effort from 2025 onwards. As a result, activities were limited mainly to WP1, WP2 and reduced scope in WP3–WP4. The platform has not yet been updated to reflect this change, which explains the apparent deviation.		
Port of Moerdijk	0.15	0.15	Jeroen van Venrooij
	Main contributions during the reporting period: Main contributions during the reporting period : Together with partners we made 10 types of harbour-specific scenario's and get it live on 20 camera's. In total we are at the moment working at scenario's on 48 camera's across the port area. We provided in 2 pilot locations (Appelzak area and Plaza parking). For the last pilot we organised 2 day-sessions: replay anomalies for training AI models and adjusting POM scenarios.		
	Discrepancy explanation: -		
Macq	3.00	3.22	Geert Vanstraelen
	Main contributions during the reporting period: Improvements on camera time synchronisation and displacement monitoring. Platform integration of real time database (clickhouse) and data analysis databases (Parquet). Pose estimation of vulnerable Road Users in the context of mobility but also intrusion into place they are not supposed to be (use case description).		
Airobot	0.66	1.75	Jan Leyssens
	Main contributions during the reporting period: No contributions for 2025 Semester-1.		
	Discrepancy explanation: Vlaio have already paid the AiRobot based on this effort number (1.75).		
Port authority	0.15	0.15	Markku Juhani Rautio
	Main contributions during the reporting period: In 2025-1, the Port Authority's main contributions were providing test sites and infrastructure, defining requirements, enabling iterative		

	validation of multi-modal AI systems, facilitating data integration, and acting as a reference demonstrator for future exploitation.
	Discrepancy explanation: No discrepancy.

4.3.2. Actual vs. planned effort overview

Report	Planned effort up to reporting period (PY) - total: 186.81 PY	Reported actual effort up to reporting period (PY)
2025 Semester 1	95.47 (51% of total)	76.31
2024 Semester 2	59.39 (32% of total)	41.62
2024 Semester 1	31.37 (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.