ITEA 4

Project Profile

SINTRA

Boosting safety and security with multi-modal sensing and AI-powered data analysis

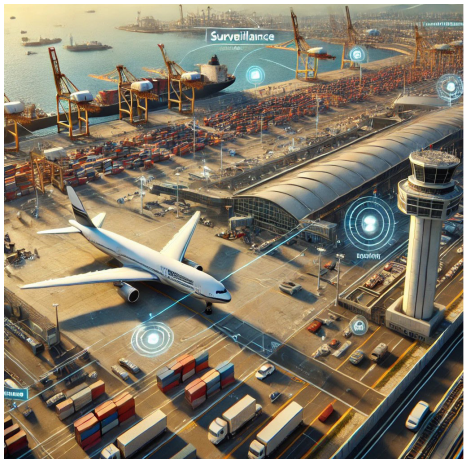
To protect critical infrastructure, the ITEA project SINTRA (Security of Critical Infrastructure by Multi-Modal Dynamic Sensing and AI) will develop an open data streaming platform that enables interoperability, information sharing and privacy protection via multi-modal sensing and AI-powered data analysis.

Addressing the challenge

Stakeholders of critical infrastructure face diverse safety and security threats, including organised crime and low-level actions like vandalism. Current security monitoring and protection systems are generally insufficient; issues include poor interoperability, minimal cross-coordination and data exchange between security organisations and weak compliance with privacy laws. This leads to localised deployments and fragmented situational awareness for operators. Additionally, reliance on video analysis opens the door to human error and limits detection to simple incidents, failing to identify high-impact, context-dependent threats like trafficking.

Proposed solutions

SINTRA will overcome these limitations by developing an open data streaming AI platform that enhances cross-organisational interoperability and trust. This will advance beyond the state of the art by integrating multi-modal sensing and AI-powered data analysis, combining various sensor inputs with existing data sources to provide a comprehensive view of infrastructure security. Prior to analysis, the input data will be processed by a data governance and trustworthiness layer that ensures data security, privacy protection and ethical requirements. AI-based analysis of the combined data will then enable robust detection of complex anomalies and map them to threats. The results and the governed-for-privacy data will be visualised on a dashboard featuring alarms, notifications and localisation, rendering all important information on a small number of displays to reduce human error. This dashboard will also support data sharing and cross-coordination among stakeholders. The benefits will be demonstrated for five critical infrastructure types: logistic hubs, airports, harbours, construction sites and shopping centres.



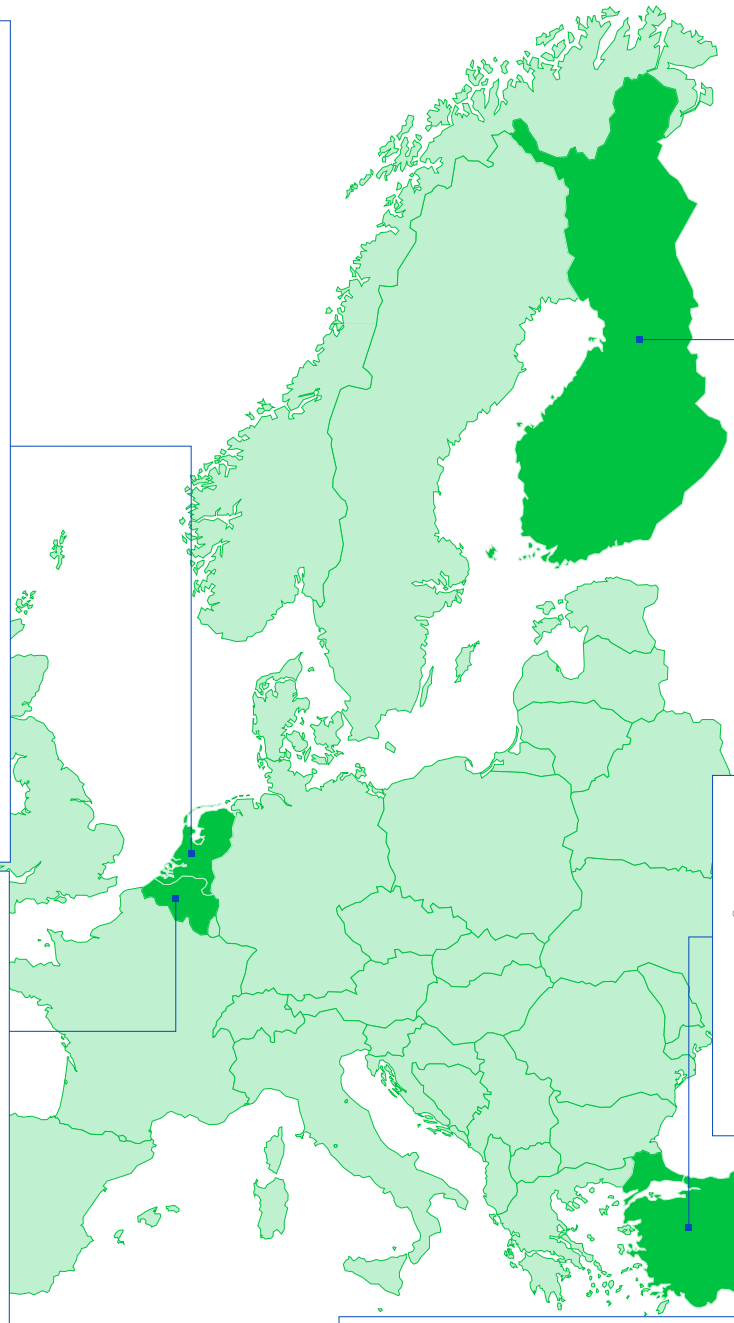
Images symbolising the SINTRA project, protecting critical infrastructures

Projected results and impact

By providing operators with a means for timely cross-coordinated response, contingency or mitigation actions, SINTRA's ultimate goal is to reduce the threat and costs of attacks. To achieve this, the project intends to reduce the current average false alarm rate from 80% to 30% and missed anomaly/threat rate from 60% to 20% while improving incident detection time by 10%. The expected business impact is threefold. First, a methodology for privacy-preserving AI-based security systems will enable large-scale business growth in the analysis-based security industry, which is stagnating due to rising legislation barriers on data collection and usage in machine learning. Second, with an open platform architecture designed for easy, dynamic integration of new sensors, analysis tools and communication protocols, SINTRA aims to reduce partner maintenance and technology upgrade costs by up to EUR 120 million annually. Finally, and most importantly, the project will allow partners to enter the emerging market of full-fledged security and monitoring solutions, with additional revenues estimated at EUR 400 million per year. By actively engaging with citizens, authorities and external stakeholders to stimulate acceptance and validate scalability, SINTRA intends to maximise its impact on the future of safety and security.

Project partners

SINTRA
22006



The Netherlands

Avular
BOSCH
TU/e EINDHOVEN UNIVERSITY OF TECHNOLOGY
MantiSpectra
omines
PORT OF MOERDIJK
SafeCity
Sorama make sound insightful
ViNotion Making surveillance smart

Belgium

AIRobot
SITE
CITYMESH the art of connectivity
Macq traffic & automation
sensolus
sirris
SKYEBASE Drone Inspection Services

Finland

ABLOY
HOXHUNT
jamk
KEMIN SATAMA Port of Kemi
secapp
2NS Second Nature Security
SENSOAN
TELESTE
JYVÄSKYLÄN YLIOPISTO UNIVERSITY OF JYVÄSKYLÄ

Türkiye

ALPATA TEKNOLOJİ
ARDGRUP
koçtaş
inosens
KoçSistem
TAV TECHNOLOGIES

Project funded by

VLAIO
innoviris .brussels we fund your future
Rijksdienst voor Ondernemend Nederland
TÜBİTAK

Project start
January 2024

Project end
December 2026

Project leader
Gökhan Koç, TAV Technologies

Project email
gokhan.koc@tav.aero

Project website
https://sintra-ai.odoo.com/

ITEA is the Eureka RD&I Cluster on software innovation, enabling a large international community of large industry, SMEs, start-ups, academia and customer organisations, to collaborate in funded projects that turn innovative ideas into new businesses, jobs, economic growth and benefits for society. ITEA is part of the Eureka Clusters Programme (ECP).

https://itea4.org

ITEA 4
eureka