Project No

**101007273**

# DAIS: Distributed Artificial Intelligent Systems

Funding Programme

**Horizon 2020 - Key Digital Technologies Joint Undertaking (KDT JU)**

Budget

**€ 32.726.240**

Project Start Date

**01.05.2021**

Project End Date

**30.04.2024**

Coordinator

**Research Institutes of Sweden**

Partners

**SESTEK & 45 more partners**

# Objectives

DAIS – Distributed Artificial Intelligence System, a pan-European effort with 47 partners from 11 countries, aims at creating intelligence-centered heterogeneous distributed edge computing systems and solutions.
DAIS's approach is to provide trustworthy connectivity and interoperability by bringing the Internet of Things and Artificial Intelligence together in a distributed edge system for industrial applications. The project will feature a large variety of industry-driven use cases embedded into the application domains, Digital Life, Digital Industry, and Smart Mobility.

**The project aims to:**

- Develop edge AI electronic components in hardware that are self-organizing, energy efficient, and private by design. The DAIS project includes research and innovation in hardware that is both digital and analog.
- Develop edge AI software that is self-organizing, energy efficient, and private by design.
- Securely integrate edge components to cloud and fog.
- Encompass three key areas: the orchestration and coordination of AI tasks running in different parts of the topology, the research in distributed security and privacy measures, and solving networking and communication needs for these highly distributed solutions.
- Demonstrate industrial AI tasks running on DAIS components.
- Support the use of existing and the emergence of new DAIS related standards based on the technical capabilities developed in the project.

# SESTEK's Ambition to be a Part of This Project

SESTEK is a B2B company that primarily provides solutions in the finance, telecommunications, and insurance sectors. The related customer cartel usually requires online systems that transfer the data to a central location and process it there. Since SESTEK aims to reach different verticals like consumer electronics, robotics or automation systems usually require processing of the data on IoT devices rather than a central location. Sestek wants to establish itself in the sectors mentioned by being part of DAIS. SESTEK embraces the opportunity to adapt its

existing solutions flexibly to these cases by benefiting from distributed AI and edge computing. DAIS gave a momentum for industrial competitiveness by locating its technologies to embedded applications combined with security aspects and processing load.


# Project Rationale

- The growing demand for employing Artificial Intelligence (AI) at the edge is evident.
- AI applications, particularly those using machine learning such as deep learning algorithms, are being propelled by advancements in models, computing capacity, and vast datasets.
- In safety-critical applications such as autonomous vehicles, face recognition, and speech recognition applications where milliseconds matter, intense time demands are required.
- Europe is not dominating in the fields of edge computing and distributed AI development and production. In this context, the EU-funded DAIS project assists Europe in assuming a more impactful role in the future of edge computing and intelligence.
- Moving AI functions from cloud-based systems to edge computing is highly esteemed in both industry and academia.

# SESTEK’s Role and Achievements

- SESTEK has created and showcased AI-enabled components designed for both cloud and edge environments, enabling their versatile utilization in various applications, such as enhancing digital experiences. These components specialize in speech and text processing, offering reliable and effective functionalities for a wide range of use cases.

- To implement the wake word detection task in a secure manner, the Federated Learning Framework Flower was used on a portion of the HeySnips Dataset.

- Taking into consideration that the model will be run on low-resource devices, the MobileBERT model was used to carry out the embedded sentiment analysis task. The resulting model achieved %85.71 accuracy on the test set.

- The way the audio spoofing problem was handled and the reliability of results from the literature have been examined. The contributions to the literature can be summarized as showing that it is possible to detect different types of attacks with a single model, combining models that give successful results in different attack types with hybrid architectures can increase performance, the effect of the reliable class in the training data on the generalization performance, and the data enrichment methods can significantly increase the performance.

- For speaker recognition, in recent experiments, the neural network that tries to map short utterance x-vectors to long utterance x-vectors improves the verification performance as EER is reduced from 8.37% to 7.67% percent.

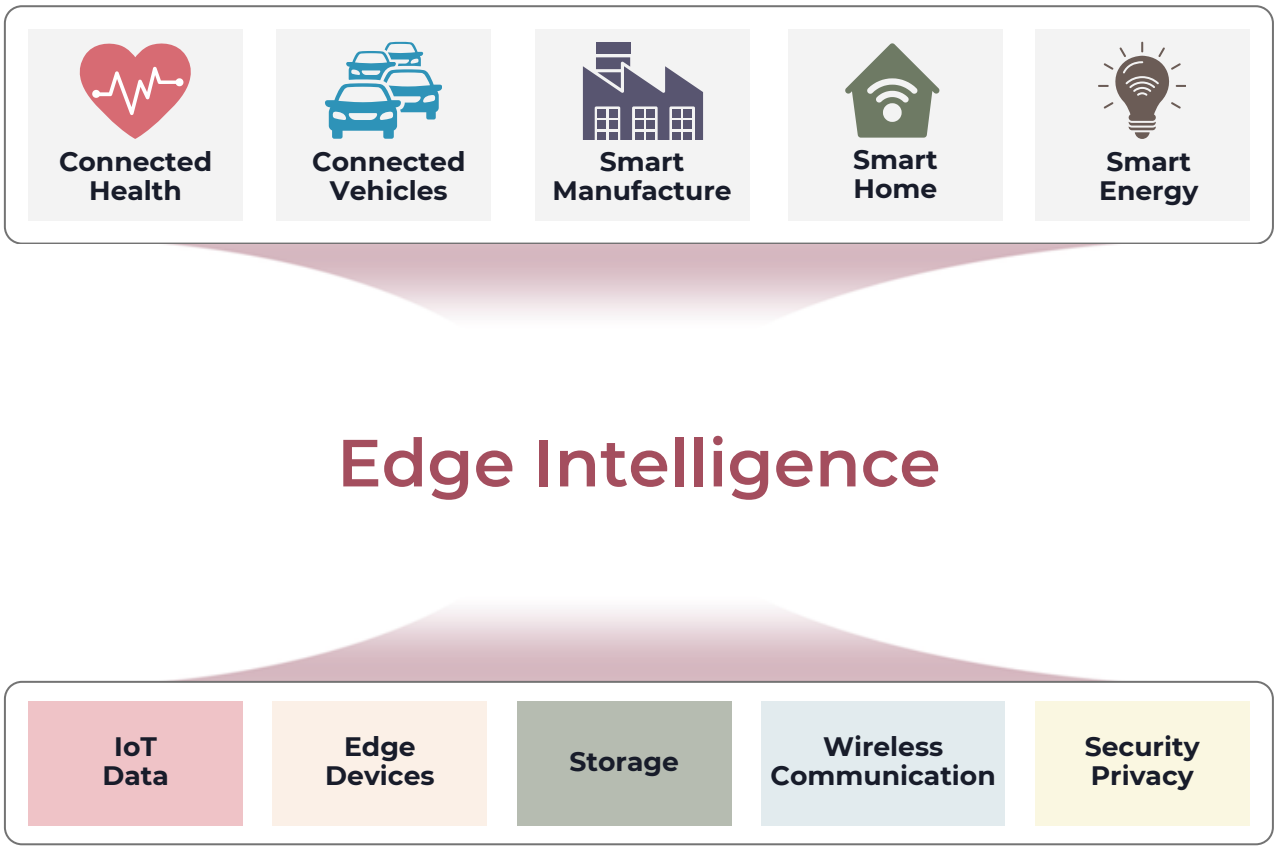
- Data augmentation has been experimented with (random background speech, noise, music augmentation, random reverberation, different audio formats augmentation) to adapt acoustic models to different conditions, increase training data volume, and avoid overfitting.

- Distributed training is applied, and in order to evaluate the impact on speaker recognition, SESTEK reduced the available bandwidth and monitored the resulting elapsed times.

- SESTEK plays a crucial role in Demonstrator 7.2, a "Privacy-Preserving Distributed Personal TV Recommendation System" that integrates the user's current mood, running on DAIS components. SESTEK contributes by incorporating its advanced speech and text processing modules into the demonstration.

- Speech recognition and sentiment analysis modules have been compiled for the Akım Metal edge hardware, which includes NXP’s card. Initial tests have been conducted by deploying and running these modules on the device.

# DAIS Schema


Connected Health
Connected Vehicles
Smart Manufacture
Smart Home
Smart Energy
Edge Intelligence
IoT Data
Edge Devices
Storage
Wireless Communication
Security Privacy