ALIF
SEMICONDUCTOR

Enhancing Driver Safety in Modern Vehicles with Alif Ensemble MCUs

A driver in a vehicle with driver safety and assistance features

The integration of AI into modern vehicles presents a transformative approach to enhancing driver safety and passenger comfort. By merging ML capabilities and sophisticated camera technologies, automakers are not only enhancing safety but contributing to a more intuitive and personalized driving experience. This case study explores the implementation of AI-enabled cameras and sensors in vehicles, focusing on Driver Monitoring Systems, Cabin Monitoring Systems, and Gesture Recognition and Life Presence Detection Systems. It also delves into the need to adopt a multi-layered approach for ensuring AI model/data security.

The Evolution of Driver Safety: From Basic Protection to AI-Enhanced Accident Prevention

Historically, vehicle safety has evolved from basic seat belts to more sophisticated systems like airbags and antilock braking systems. Today, driver safety features have expanded to include preventive technologies that can anticipate and mitigate risks before they lead to accidents. AI-enabled cameras, with their ability to detect and interpret visual cues, are key components of this evolution.

Unlike standard camera systems, AI-assisted cameras perform sophisticated image processing via advanced algorithms for tasks like object detection, classification, and tracking. Techniques like convolutional neural networks (CNNs) and deep learning are a few of the latest technologies being used for these purposes, allowing in-vehicle cameras to interpret visual data more accurately and in real-time.

Below is a look at some of the latest driver safety features for modern automobiles:

Driver Monitoring

A critical component in modern vehicles for increasing driver safety is the Driver Monitoring System (DMS). This system uses AI and a sophisticated camera setup to monitor a driver's state. The DMS continuously observes the driver's facial expressions and eye movements. If signs of distraction – such as prolonged lack of focus on the road – are detected, the system can issue alerts via sound or displays on the dashboard. For drowsiness monitoring, a DMS analyzes blinking patterns and head positioning to identify signs of fatigue. It then alerts the driver, suggesting breaks when necessary. Moreover, the DMS can identify a driver by facial features, allowing for personalized settings in the vehicle.

Cabin Monitoring

The Cabin Monitoring System (CMS) takes passenger safety and comfort to new heights. Using cameras and sensors, the CMS not only monitors but also responds to passengers' needs. For example, In semi-autonomous or autonomous vehicles, the CMS helps ensure that passengers are properly seated, a critical factor for toggling on autonomous driving modes. The CMS employs camera sensors to understand human behavior and detect movements within the vehicle. It then adjusts elements such as the air temperature or driving mode, enhancing passenger comfort. Before an accident occurs, the CMS can intelligently adjust the intensity and timing of airbag deployment to reduce the risk of injuries.

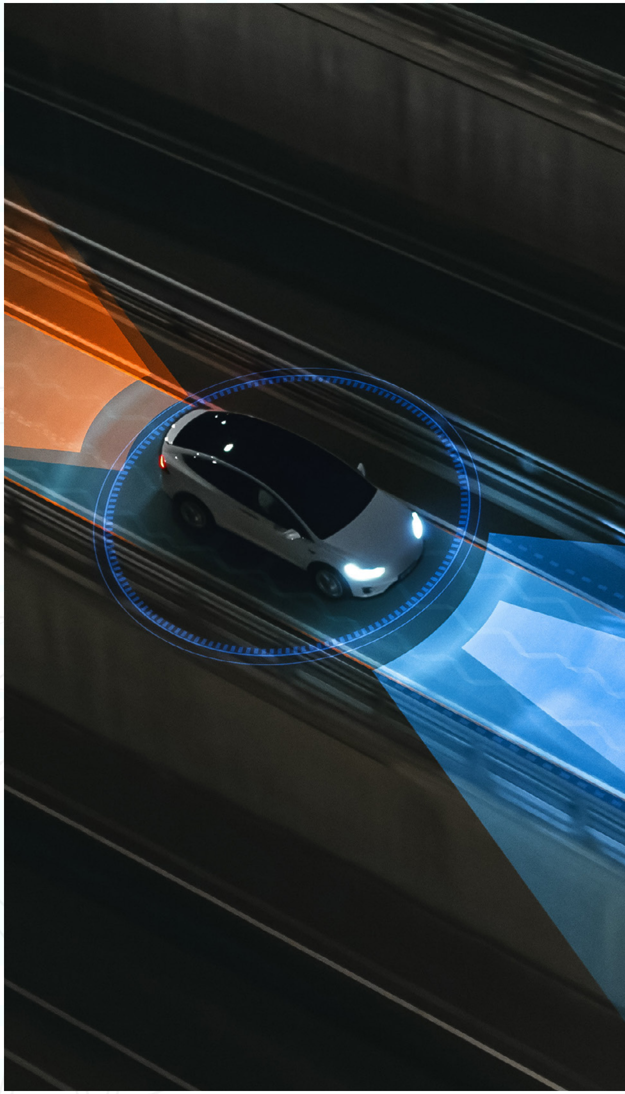
Gesture Recognition and Life Presence Detection

Gesture detection and life presence detection systems represent a fusion of ML algorithms and cutting-edge Time of Flight (3D) cameras. The system enables intuitive interaction with the vehicle through gestures, making the driving experience more seamless and focused. For example, life presence detection systems play a crucial role in preventing tragic incidents by detecting the presence of children or pets left unattended in the vehicle. This system is crucial in preventing heat stroke or hypothermia in vulnerable passengers.

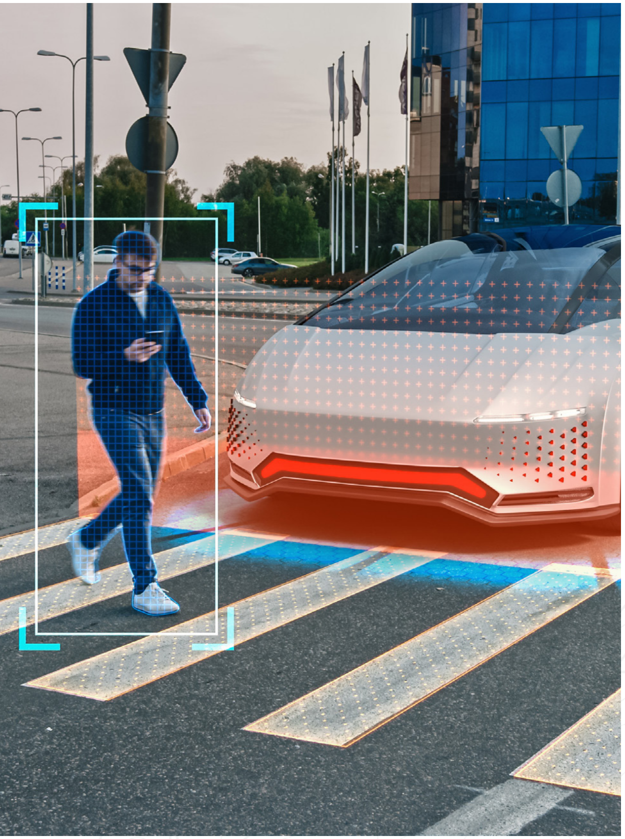
Securing AI in Automotive Technology: Proactive Strategies for Data and Model Protection

Given the complexity and sensitivity of the data and models utilized in automotive applications, a multi-layered approach to ensuring data security is essential. As AI models are increasingly fine-tuned and customized, the risk to sensitive and confidential data is evident. Automakers can take a forward-looking approach to ensure the integrity and confidentiality of these models, protecting them against both external threats and internal vulnerabilities.

The integration of AI/ML in vehicles, particularly in systems like Driver Monitoring Systems, Cabin Monitoring Systems, and Gesture Recognition and Life Presence Detection Systems, also brings about challenges in terms of data security. Taking a proactive stance to securing AI models and data that drive these systems will be critical for automakers in the long term. This involves protecting AI models from being tampered with or reverse-engineered. The data used by DMS, for example, such as training facial features for driver identification, is sensitive and must be protected both at rest and in transit.



AI car camera. Photo credit: Adobe Stocks



AI car camera. Photo credit: Adobe Stocks

Secure encryption and storage techniques are essential to prevent unauthorized access.

The CMS, which adjusts vehicle settings based on occupant behavior and needs, also handles sensitive data. Automakers must take security measures to ensure that personal preferences and behavioral patterns of the occupants are not vulnerable to unwanted access. This requires robust encryption protocols and real-time monitoring to detect and prevent unauthorized access or anomalies during data transmission. Similarly, security measures in Gesture detection and life presence detection systems must focus on protecting the integrity of the gesture recognition algorithms and the data they process. The security requirements for these systems extend to the AI models themselves.

The protection paradigm spans three principal states of code and/or data:

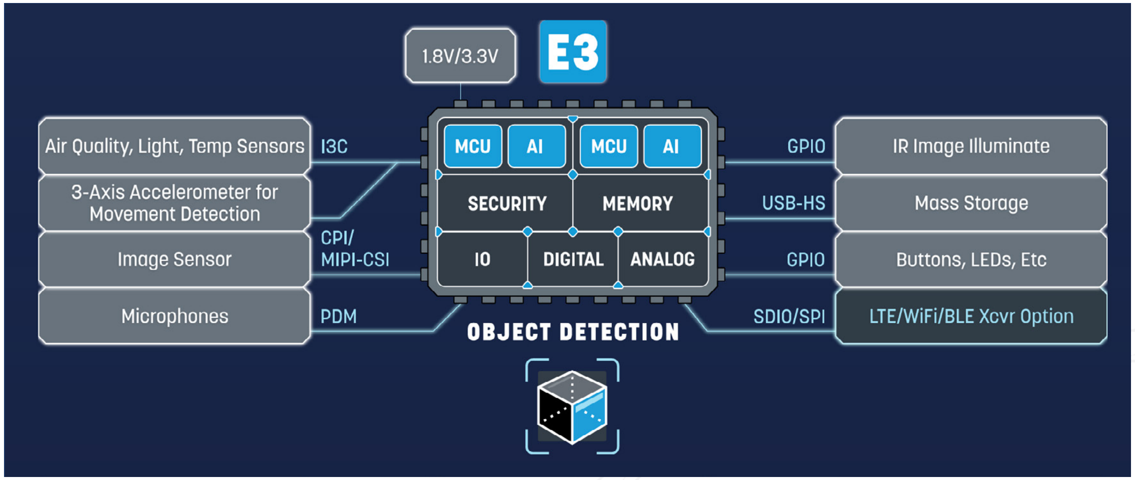
- At Rest: Ensuring that AI models and their data are securely stored locally, using encryption and access controls.
- In Transit: Protecting the transmission of AI models and their data, which involves secure communication protocols and data encryption.
- During Execution: Protecting AI models from attacks during runtime. This includes measures to avoid reverse engineering or extraction of model features and training datasets, which could be exploited for malicious purposes.

The Role of MCUs and MPUs in Computer Vision for Automotive Applications

Microcontrollers (MCUs) and Microprocessors (MPUs) are at the heart of embedded systems in modern vehicles which enable DMS, CMS, and Gesture recognition/Life Presence Detection systems. They are responsible for processing the data from camera sensors, running algorithms to detect and analyze objects, and making decisions based on the analysis. For example, CMS and DMS utilize sophisticated machine learning models such as support vector machines (SVMs) and recurrent neural networks (RNNs) for pattern recognition and behavioral prediction.

These models are trained on vast datasets to recognize a wide range of human expressions and behaviors, enhancing the sensitivity and accuracy of camera sensors. Gesture recognition systems use complex algorithms like Hidden Markov Models (HMM) and Dynamic Time Warping (DTW) to recognize human gestures. Each system must be highly responsive and accurate to correctly understand the driver's commands without causing distractions.

Enhancing AI/Data Security with Alif's Ensemble Family



Alif's Ensemble family of 32-bit embedded processors make available single-core and dual-core devices using Arm® Cortex®-M class MCUs with optional micro Neural Processing Units (NPUs) for AI/ML acceleration, and continue on with triple- and quad-core fusion processors that add Cortex-A class MPUs -- essentially combining MCUs and MPUs into a single device.

In general, the performance and efficiency of Alif MCU devices exceed the performance of traditional MPUs for AI/ML workloads, and as a result the system becomes smaller, more power-efficient, and less costly. The Ensemble E3 dual-core MCU shown above is an optimum choice enabling precise object and event classification as well as increased accuracy in person detection, gesture recognition, optical character recognition, and sensors data fusion for driver safety.

Alif's aiPM™ technology also provides efficient power management to extend battery life and ensure maximum uptime.

All Ensemble family devices employ various mechanisms to defend against a range of threats that include authentication-based defense, OOD feature learning, bot management, and prompt engineering.

Strong Authentication-Based Defense

A viable defense strategy for AI models is building a strong authentication-based system. Leveraging Public Key Infrastructure (PKI) key exchange can ensure secure authentication between the model host and service provider. This approach can prevent black-box model extraction attacks, where unauthorized users attempt to extract AI models. Alif's in-factory creation of unique device key pairs inside every device during manufacturing enables customers to enforce mutual authentication mechanisms during critical AI operations on the device and utilize its secure enclave to dynamically respond to attacks and decide on the adequate recovery options.

Out-of-Distribution (OOD) Feature Learning

An innovative defense against model extraction attacks is using Out-of-Distribution (OOD) feature learning. Attackers often use OOD data to test victim models, aiming to clone them. Alif devices can counter this by training auxiliary models on additional data to form a defense model with a confused decision boundary. When faced with attack data containing OOD features, this auxiliary model, executed on the second NPU core of Ensemble MCUs, produces predictions that hinder the construction of the decision boundary of the training data.

Bot Management

To counter AI model extraction through repeated queries — a tactic frequently employed by attackers — bot management systems are vital. These systems are designed to detect and mitigate automated interactions with AI models. To be deployed on the second NPU subsystem, bot management obscures the true behavior of the models from attackers, thus thwarting attempts at model extraction or replication through querying.

Prompt Engineering

Another layer of defense Alif employs is prompt engineering, which involves controlling the API calls or prompts that feed the NPUs. Using one of the Cortex-A cores and an Ensemble fusion processor to filter these prompts, manufacturers can obfuscate the underlying logic and parameters of the AI models. Alif's flexible firewall features can also prevent direct API access to the MCU domain hosting the model, forcing validation through the Cortex-A domain where queries can be analyzed and redirected.

A modern vehicle illustrating advanced driver assistance and safety capabilities

Conclusion

The integration of AI/ML technologies in modern vehicles marks a significant leap towards smarter, safer, and more responsive driving experiences. From monitoring driver alertness to personalizing cabin environments, these systems exemplify the potential of AI and ML in enhancing safety and passenger comfort. However, given the complexity and sensitivity of the data and models in automotive applications, proactive security measures are essential to ensure data security. A comprehensive strategy involves safeguarding the AI models and data that underpin these advanced systems. This approach is crucial to maintain end-user trust in these technologies and ensure their safe and secure deployment in automobiles.

https://alifsemi.com/

ALIF
SEMICONDUCTOR