Building secure digital systems and ECUs for smart cars

Kaspersky Automotive Adaptive Platform

kaspersky

KasperskyOS

Driving automotive cybersecurity

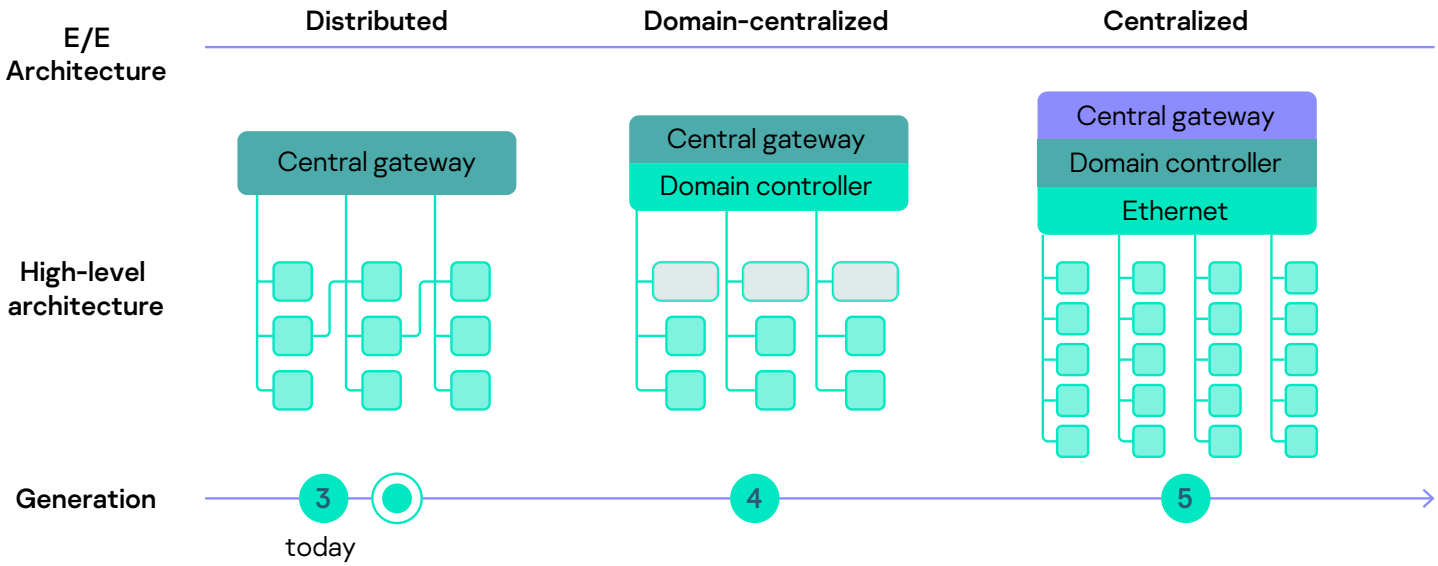
Kaspersky Automotive Adaptive Platform β* is an SDK that allows you to create secure and reliable applications for electronic control units (ECUs). It is based on KasperskyOS, a microkernel operating system used to build secure solutions for autonomous driving (HAD/ADAS), digital cockpits (TCU/V2X, gateways) and other ECU domains.

Applications created with Kaspersky Automotive Adaptive Platform conform to the AUTOSAR Adaptive Platform standard and are updatable over the air via Uptane-compatible OTA solutions.

Challenge

Autonomous, connected, electric and shared vehicles (ACES) are heavily influencing automotive industry business models. Assistance systems for semi-automated driving, regular over-the-air updates and the subsequent installation of additional software will soon become standard for many vehicles.

However, without new architectures and high-performance electronic control units (ECUs), these sophisticated electronic functions cannot be implemented. **Separation of hardware (HW) and software (SW) platforms** in next-gen electrical/electronic (E/E) architectures can help to achieve this. Such an approach will fundamentally change the dynamics of the automotive industry, its ecosystem and key players.



Source: McKinsey&Company "Automotive software and electronics 2030"

Future development of automotive E/E architecture

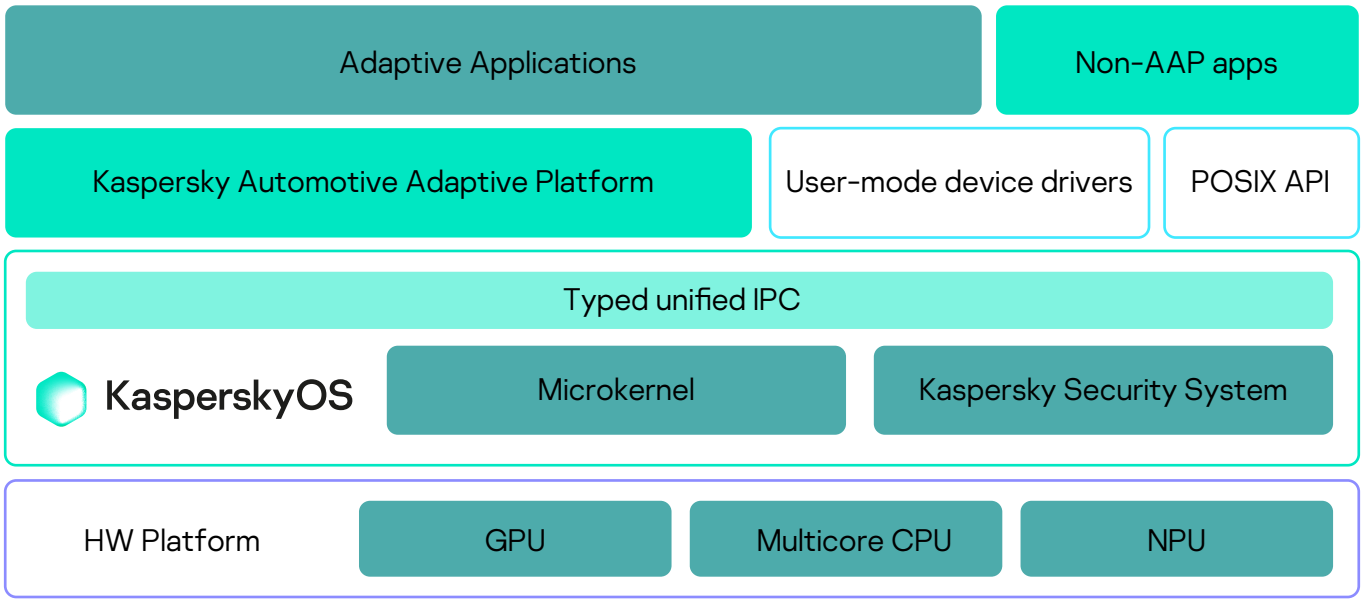
The set of strategic actions for OEMs includes a plan to control the costs of continuous HW and SW advances and to create more flexible cross-functional development. But this flexibility and updatability of safety-related software enlarges attack surfaces for malicious actors and brings new cybersecurity risks to passenger safety, data privacy and the business continuity of automotive industry players. **The changed E/E architecture and new automotive regulations require a new approach to cybersecurity.**

Kaspersky Automotive Adaptive Platform's key advantage is that it gives vendors the ability to develop complex applications for modern computing platforms independently of one another, with the focus on performance, parallel processing, interoperability and updating capabilities.

* Ready for prototyping

Kaspersky Automotive Adaptive Platform β

Within Kaspersky Automotive Adaptive Platform, Kaspersky offers a verified and validated software stack that includes **the KasperskyOS operating system, basic software, security elements and AUTOSAR Runtime for Adaptive Applications (ARA):**



Elements comprising the Kaspersky Automotive Adaptive Platform solution

Kaspersky Automotive Adaptive Platform is capable of running both Adaptive Applications as well as non-platform services. It provides the applications with AUTOSAR-compliant functional clusters, platform services, a POSIX-capability layer, as well as industrial-grade libraries and frameworks for autonomous driving systems. KasperskyOS supports modern multicore SoCs with hardware acceleration and is capable of functioning in redundant safety-integrated systems.

To simplify the porting process of the existing code (applications, third parties) to Kaspersky Automotive Adaptive Platform, it includes a special porting automation tool. It leverages the necessary checks and transformations required to adapt existing AUTOSAR Adaptive Applications, and integrates them to boot an image building pipeline. Kaspersky also provides engineering services for any type of software porting to KasperskyOS. Our dedicated driver development team is capable of implementing a board support package (BSP) for any new ECU types.

Customer benefits

Easier implementation of new business models in software and services:

- Service-oriented architecture establishes clear separation of software from different suppliers on one ECU;
- Continuous secure update capability over the entire vehicle life cycle in the field.

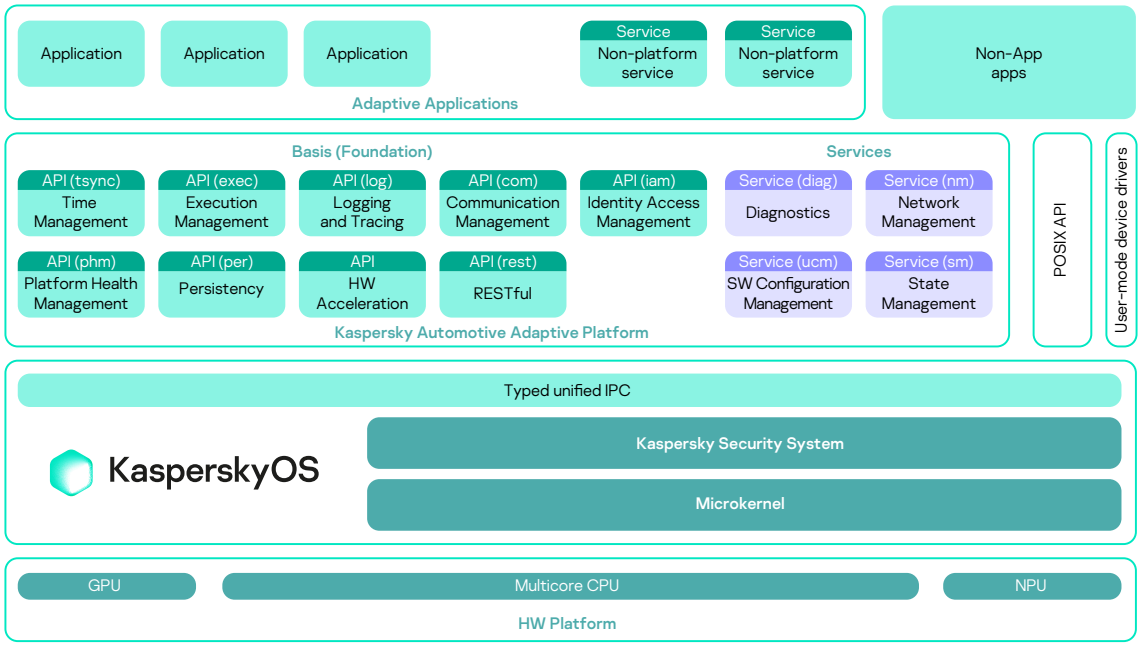
Significant time and cost reductions:

- Simple integration of connected and automated driving applications via a standardized software framework;
- Simple, fast and secure over-the-air addition of new functions during the car's life cycle;
- Quick start-up with sample projects included.

The vendor can focus solely on functional development; cybersecurity and standards interoperability are our responsibility.

Functional clusters and platform services

- Kaspersky Automotive Adaptive Platform provides AUTOSAR-compliant functional clusters and platform services.
- Both non-AUTOSAR apps and Adaptive Applications can use ISO/IEC 9899:1999 and/or the POSIX compatibility layer.
- PSE51 and PSE52 POSIX 1003.13 profiles are fully supported. The POSIX 1003.1 standard is also partially supported, with the most notable limitation being the absence of process control primitives (such as fork() and exec()).
- Industrial-grade libraries and frameworks for autonomous driving systems (OpenCV, Point Cloud Library, FLANN) are also provided.
- The AUTOSAR platform provides C++11 (ISO/IEC 14882:2011) interfaces, and also supports various communication (SOME/IP, DDS, e2e, e2exf, REST) and diagnostic protocols (UDS/DoIP, DLT).



Kaspersky Automotive Adaptive Platform function clusters and services overview

Features

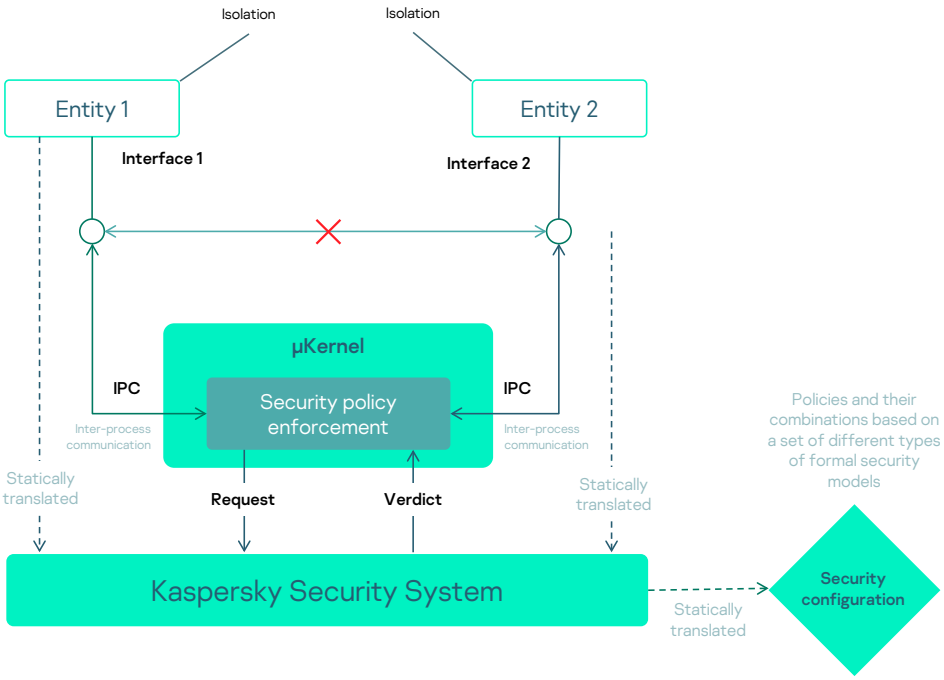
Most operating systems consider security to be a matter of separating and controlling access to system resources. Unlike those operating systems, KasperskyOS extends this scope with capabilities to specify and enforce solution-specific security properties.

Only a bare minimum set of functions is considered to be trusted, while other components are not trusted and may contain problems and vulnerabilities of some kind. Using KasperskyOS and Kaspersky Security System (KSS), security properties are defined and enforced for the whole system. Even if a vulnerability is exploited in one of the untrusted components, it won't affect the whole solution and won't damage critical functions.

The following is an overview of KasperskyOS security concepts and mechanisms:

- **Microkernel.** Based on an in-house microkernel, not a modification or improvement on an existing OS. Minimal amount of code lines necessary to make kernel mechanisms work, providing more control over the OS code quality.
- **Secure by design.** Developed on MILS principles and integrating a flexible access control system (KSS).
- **Strong isolation.** The system guarantees isolation of security domains and separation of security features from functional components.

- **Unified inter-process communication (IPC) mechanism.** The microkernel provides a single IPC mechanism.
- **Explicitly defined typed interfaces.** Every service must statically declare all provided interfaces. KSS verifies the correctness of all IPC messages based on interface declaration.
- **Static security configuration.** All processes and their permitted types of communication are preconfigured and checked before functioning.
- **Complete mediation.** The microkernel intercepts all inter-process communications and checks with KSS, which calculates access decisions based on the security configuration.
- **Default Deny.** Any action that is not preconfigured in the security policies is denied by default.
- **Remote Procedure Call protection.** Security policy implementation for service-oriented distributed architecture (Avatar scheme) for SOME/IP in AUTOSAR Adaptive.



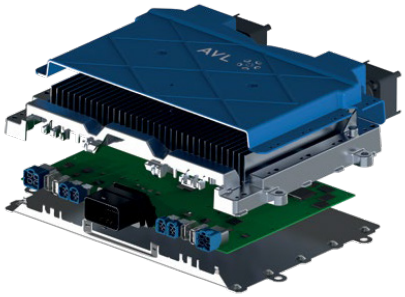
KasperskyOS core security principles

Case studies

In summer 2020, Kaspersky announced the first successful integration of Kaspersky Automotive Adaptive Platform **into the electronic control unit (ECU) of an auto-pilot system developed by AVL Software and Functions GmbH (AVL SFR)** named AVL Ajunic.

AVL Ajunic is an advanced driver assistance system (ADAS) controller, an open, customizable development platform for both prototype and series development that is also safe and secure by design, as its SoCs run on KasperskyOS. This secure operating system protects communications between ADAS components and safeguards all autonomous vehicle functions. As part of the security feature, KasperskyOS guarantees that undeclared functionality – either unnoticed at launch or inserted during system updates – cannot be exploited and will not affect the performance of autonomous vehicles.

The OS platform leverages the hardware capabilities for various ECU use cases: camera and other sensor processing, internal/external storage, CAN and Ethernet in-vehicle connectivity, power-supply control, various buses (CSI-2/RGMII/SPI), etc.



AVL Ajunic electronic control unit

About Kaspersky

Kaspersky is a global cybersecurity company founded in 1997. Kaspersky's deep threat intelligence and security expertise is constantly transforming into innovative security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe.

The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Kaspersky also advances the development of Cyber Immune solutions based on its own operating system, KasperskyOS. Such solutions are innately secure against the overwhelming majority of cyberthreats, both known and unknown.

Over 400 million users are protected by Kaspersky technologies and we help 250,000 corporate clients protect what matters most to them.

Learn more at www.kaspersky.com and os.kaspersky.com

About AVL Software and Functions GmbH

AVL is the world's largest independent company for the development, simulation and testing of powertrain systems, their integration into the vehicle as well as new fields like ADAS/AD and Data Intelligence.

AVL Software and Functions was founded in 2008 and has been experiencing strong growth ever since. It develops technologically leading software and system solutions for intelligent and ecologically compatible mobility as well as system integration and electronics development.

Based on strong technical knowledge, AVL SFR cooperates with customers and partners like Kaspersky worldwide, finding comprehensive solutions together. The company's focus is on fuel-saving topics, performance optimization and pollutants minimization for classic drive concepts and increased efficiency for e-mobility applications, as well as safety and security applications and digitalization services.

Learn more at www.avl-functions.com

KasperskyOS

Kaspersky Automotive Adaptive Platform

Learn more on os.kaspersky.com

www.kaspersky.com