Secure Communication Unit

AVL and Kaspersky Lab present their SCU innovation for tomorrow's cars – featuring enhanced diagnostic technologies via over-the-air (OTA) links

The number of ECUs and system complexity can be expected to increase at an unprecedented rate.

In the world of technology there are more than 60 available assistance systems for passenger vehicles, which help to prevent traffic accidents from happening. To enable this large range of assistance functionality, modern cars contain up to 80 electronic control units (ECUs) and a variety of network platforms. Looking at the functionality of future Advanced Driver Assistance Systems (ADAS), the number of ECUs and system complexity can be expected to increase at an unprecedented rate.

Faced with this level of variety and complexity in automotive system design, the time and effort associated with building system applications, as well as the corresponding testing and validation costs, will also increase significantly. This will lead to an uneconomical development process.

It is necessary to improve the control units already installed in cars, and also constantly monitor software operations, to find and fix any possible problems that may otherwise put drivers seriously at risk. Improvements must be made constantly, and as soon as possible, in order to avoid safety issues.
To achieve these targets, more flexible update mechanisms are needed, along with configurable data collection for many systems. This means accessing vehicles for diagnostic and update purposes will not only need to take place in garages through wired connections, but anywhere via OTA links.

It is necessary to improve the control units already installed in cars, and also constantly monitor software operations, to find and fix any possible problems that may otherwise put drivers seriously at risk.

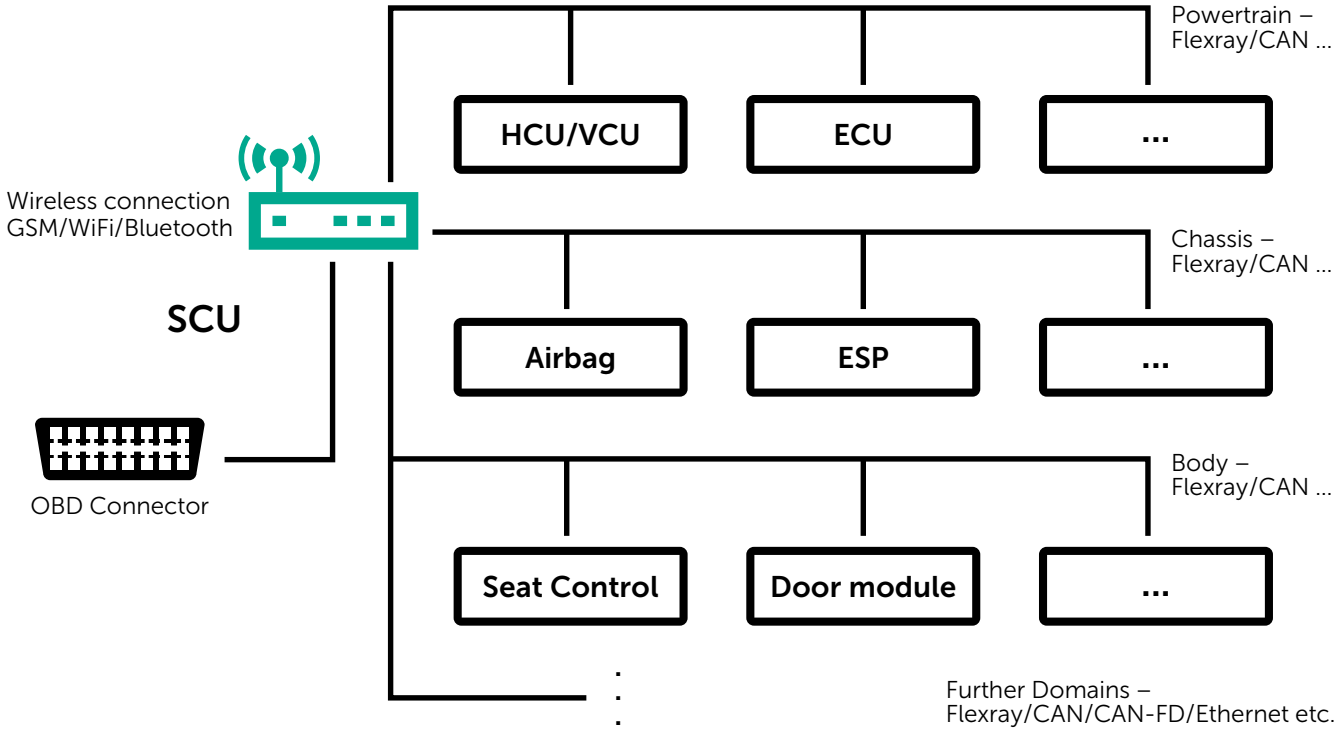
Strategic Partnership

To meet these challenges, AVL, the world's largest independent company for the development, simulation and testing of powertrain technology for passenger cars, and Kaspersky Lab, a leading global cybersecurity company, are proudly

presenting a new and innovative carrier of embedded automotive diagnostic features in synergy with reliable security solutions - as one of many possible examples of automotive connectivity.

An example of the location of the Secure Communication Unit (SCU) inside a network of automotive control units is shown below:

SCU within vehicle E/E architecture



The SCU is a communication gateway control unit, connected to several subnets and/or gateway controllers to those subnets within the car network. Thus, the SCU is a single gateway to external communications, whereas internal devices can communicate within a domain or even between domains without using SCU services.

Moreover, the SCU provides direct access to the on-board diagnostics (OBD) interface. This interface serves both as the OBD gateway for subsequent subnets and for OBD access to the SCU control unit itself. Additional connectivity is granted by wireless communication modules.

Wired implementation of the connections consists of CAN, CAN-FD, Flexray and Ethernet for in-car-connections, as well as an OBD-interface. Additionally, wireless connections are provided by GSM (up to the upcoming 5G-standard), WiFi and Bluetooth modules. The first is required for communication with the OEM backend, while the latter can be used for connections with local devices (such as consumer electronics, home networks, repair workshop testers, etc). The interfaces of the SCU are able to comply with the architecture above. That means that several connectors are available for all the wired connection types, such as CAN.

Required transmission rates are limited by the corresponding connection type only. For wired connections the benchmark correlates to Ethernet data rates, whereas wireless connections will be able to reach 5G standard performance (1Gbps).

The SCU diagnostic device can carry out the following actions

- Event audit and logging
- Authenticating external sources for access to the SCU
- Uploading the script images and data onto the SCU from external sources
- Appropriate storage management of script images and data, by remote request if needed
- Script execution following an appropriate request
- Interaction with off-board testers

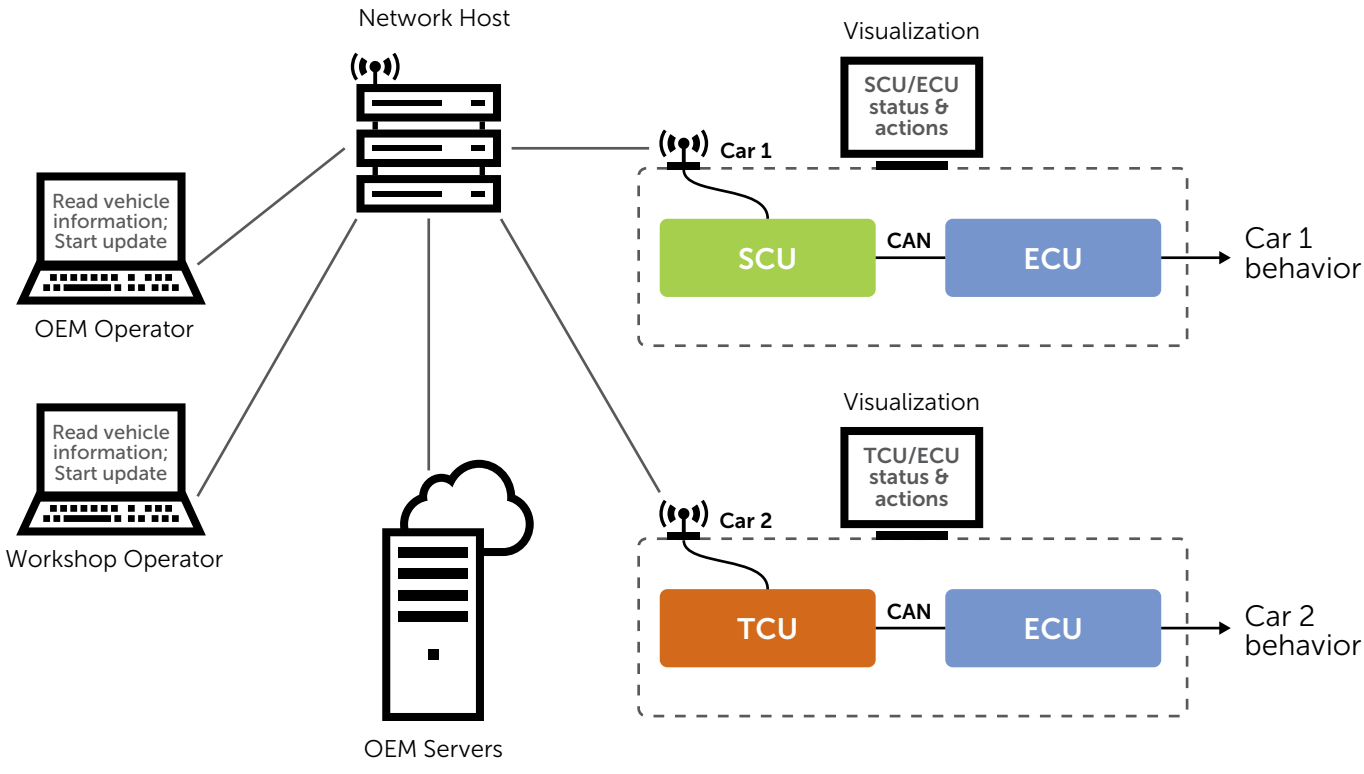
The SCU is powered by the KasperskyOS operating system and hardened by Kaspersky Security System (KSS), a security policy computing engine. KasperskyOS controls all of the interactions within SCU at the lowest level, and enforces verdicts provided by KSS. Only explicitly allowed interactions are possible.

The SCU demonstration architecture simulates a connected fleet, where some vehicles are equipped with innovative and secure SCU technology, others with unprotected telematic control units (TCU). Each vehicle network consists of a dashboard and infotainment mockup, as well as a CAN-connected ECU to control its car's behavior.

In this scenario, connectivity is achieved by a wireless network consisting of an OEM backend server, client devices for operator interaction with a frontend, and the connected cars themselves, implemented by SCU and TCU. The network host is connected by a WiFi router, which simulates the GSM-ISP.

The OEM operator is thus capable of connecting and interacting remotely with the car in the field, such as by providing secure software updates over the air or using data logging to monitor the fleet's behavior. Additionally, third-party operators from workshops or dealers, for example, may be allowed to use a subset of these features. However, only SCU is reliably able to distinghuish their roles and enforce strong security policies via KasperskyOS and KSS.

Demonstration architecture



Kaspersky Transportation System Security
39A/3 Leningradskoe Shosse, Moscow,
1252121, Russian Federation
www.kaspersky.com
transportation.security@kaspersky.com
connectedcars@kaspersky.com
Phone: +7-495-797-8700
Fax: +7-495-797-8709
+7-495-956-7000

AVL Software and Functions GmbH
Im Gewerbepark B29
D-93059 Regensburg
www.avl.com
info.rgb@avl.com
Phone: + 49 (0)941 630 890
Fax: + 49 (0)941 630 89 111