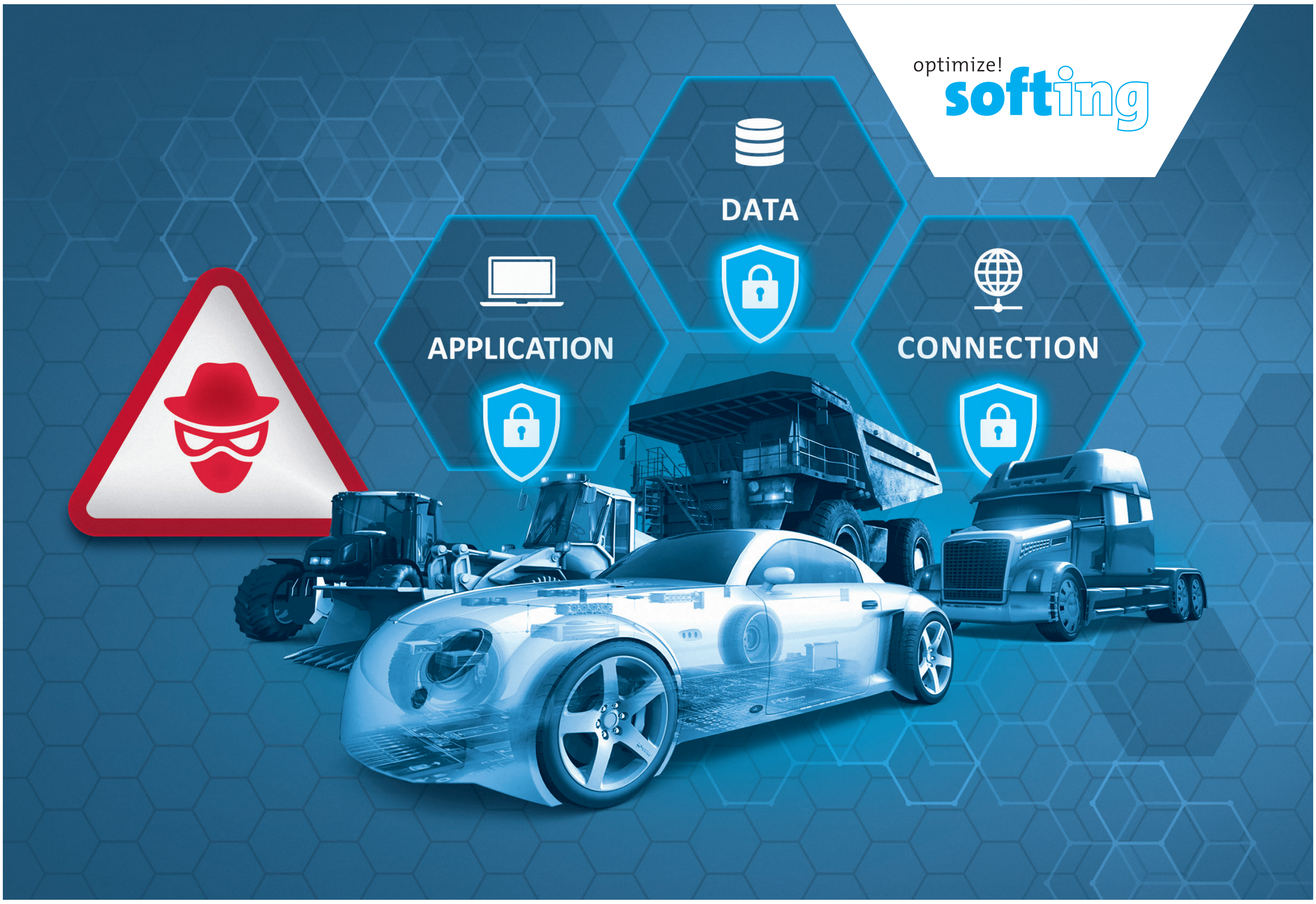

© Softing Automotive

Diagnostics and Security: Brave New World

Opportunity or risk?

Familiar truths are a little tricky – while they are practical to use for a quick appraisal, they are not eternally true! And modern vehicle diagnostics is no exception. In the past you were able to rely on the fact that a vehicle was accessed via the standardized OBD jack; also the means of communication with protocols that were also standardized – protocols which, incidentally, by design cannot fulfill important security requirements. But modern vehicles open themselves up to the outside in a number of ways. V2x (Vehicle to any environment) requires wireless communication with external devices and a SIM card is mandatory for the eCall functionality required in all vehicles today. The demand to be able to update vehicle software without having to visit the repair shop (SOTA – Software over the air) means wireless connections are also creeping into the diagnostic environment.

But that also entails risks. Unauthorized penetration of these wireless communication paths can lead to extensive damage:

- Physical injury: A hacker takes control of the vehicle; people can be injured or even killed.
- Warranty claims: Tuners modify vehicle data over the air to induce wear and tear at an early stage so parts have to be exchanged at the OEM's cost.
- Data protection: Unauthorized third parties access personal data: Current legislation means that the VIN (Vehicle Identification Number) also counts as personal data. Fines can amount to as much as 50,000 € in each case.

The press recently focused on an example of the possible extent of damage: British Airways had not secured customer data sufficiently well. The British legal system decided on a fine of 200 million €. (Spiegel Online, July 8, 2019)

Hardware and software repair

Today, the life cycle of a vehicle is simply not possible without diagnostics: Repairing a network consisting of more than 100 ECUs (Electronic Control Units), with distributed functions, is simply not possible for a mechatronics engineer in the repair shop. The following is true in manufacturing: an employee on the production line cannot determine whether a vehicle is being put together correctly at any particular point of construction. During engineering, many variables in close-to-production ECUs are no longer accessible. In all these cases, an expert system has to evaluate information which is generated and made available in the vehicle itself. Furthermore, the communication mechanisms introduced in diagnostics are also used for updating the ECU software. This is just as true in engineering, where new versions are brought in for testing, as it is in manufacturing and after sales service, where a software repair is effectively carried out with the latest version of the software.

There are three basic types of service when it comes to accessing a vehicle:

- *Reading services* are used to read out information from the vehicle. This information may be measurement values, i.e. physical values, which are used in the ECU to control functions, or error memory entries. The latter are entered by the ECU as soon as any irregularities occur in the course of continuously running self-test routines.
- *Writing services* change content in an ECU. This takes place, on the one hand, in the programming and, on the other, in the variant coding. This is used to adapt uniform ECU software to a range of behavior modes stemming, for example, from country peculiarities (steering wheels on the right or left) or for different equipment options (same engine with different power levels).
- *Executing services* enable routines to be started in the ECU. These include addressing actuators such as a wiper motor alongside test functions. Using diagnostics, no switch is necessary for example on test benches.

Today the vehicle is usually accessed via two bus systems: In the classic form over CAN with the UDS (Unified Diagnostic Services) protocol or over Ethernet with Diagnostics over IP (DoIP).

Gateways…

As long as diagnostics takes place locally, in other words using a cable connection between the diagnostic tester and the diagnostic interface or the vehicle, it is safe to assume that the diagnostic system is basically secure as far as unauthorized access is concerned. But the picture changes as soon as there is a remote data connection over the Internet:

A remote diagnostic connection with the vehicle is established by the user after the application is started and the vehicle has been selected. Generally, the Internet is used as the transport layer. This connection is used to send the relevant service requests to the vehicle which, all things being equal, sends the relevant responses. Once the data requested has been received, the tester application evaluates it

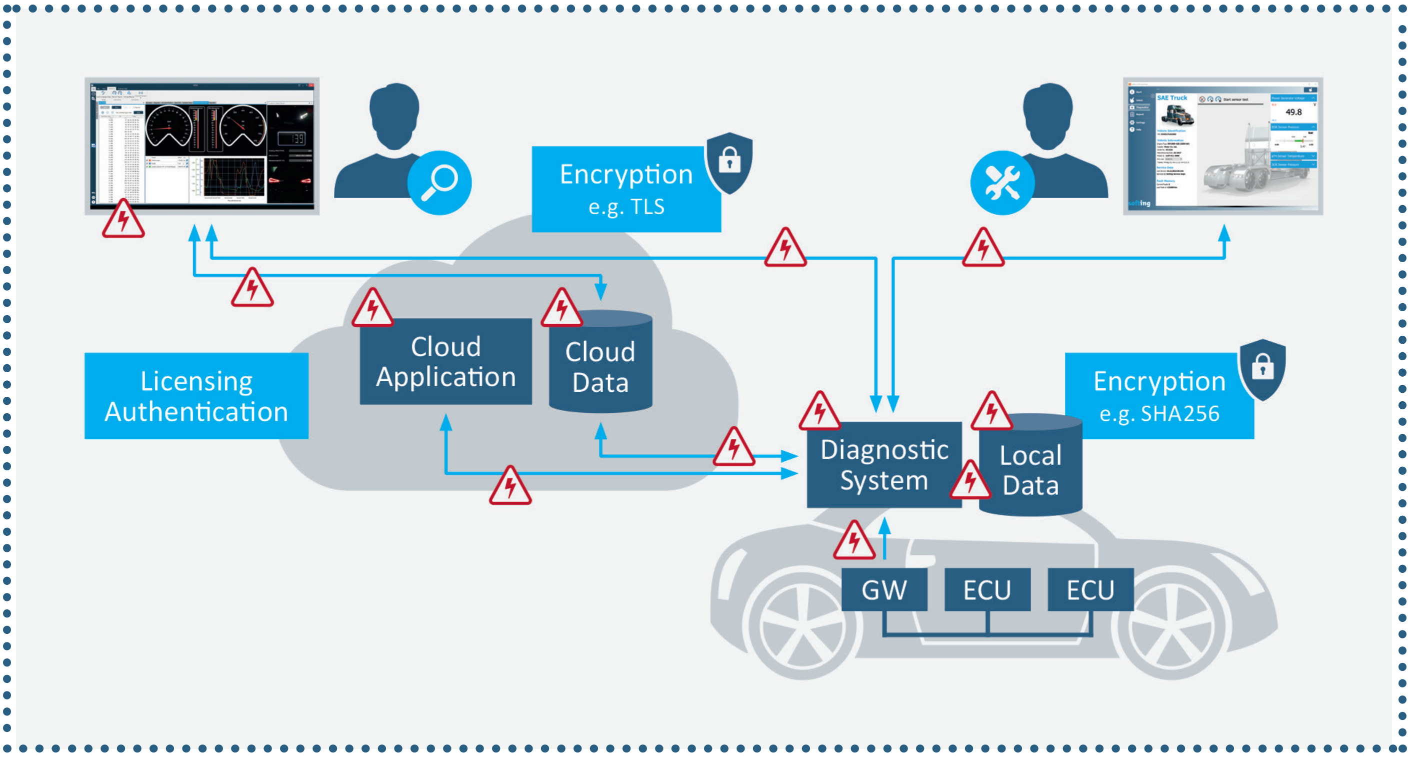

Figure 1: The Diagnostic Ecosystem
(© Softing Automotive)

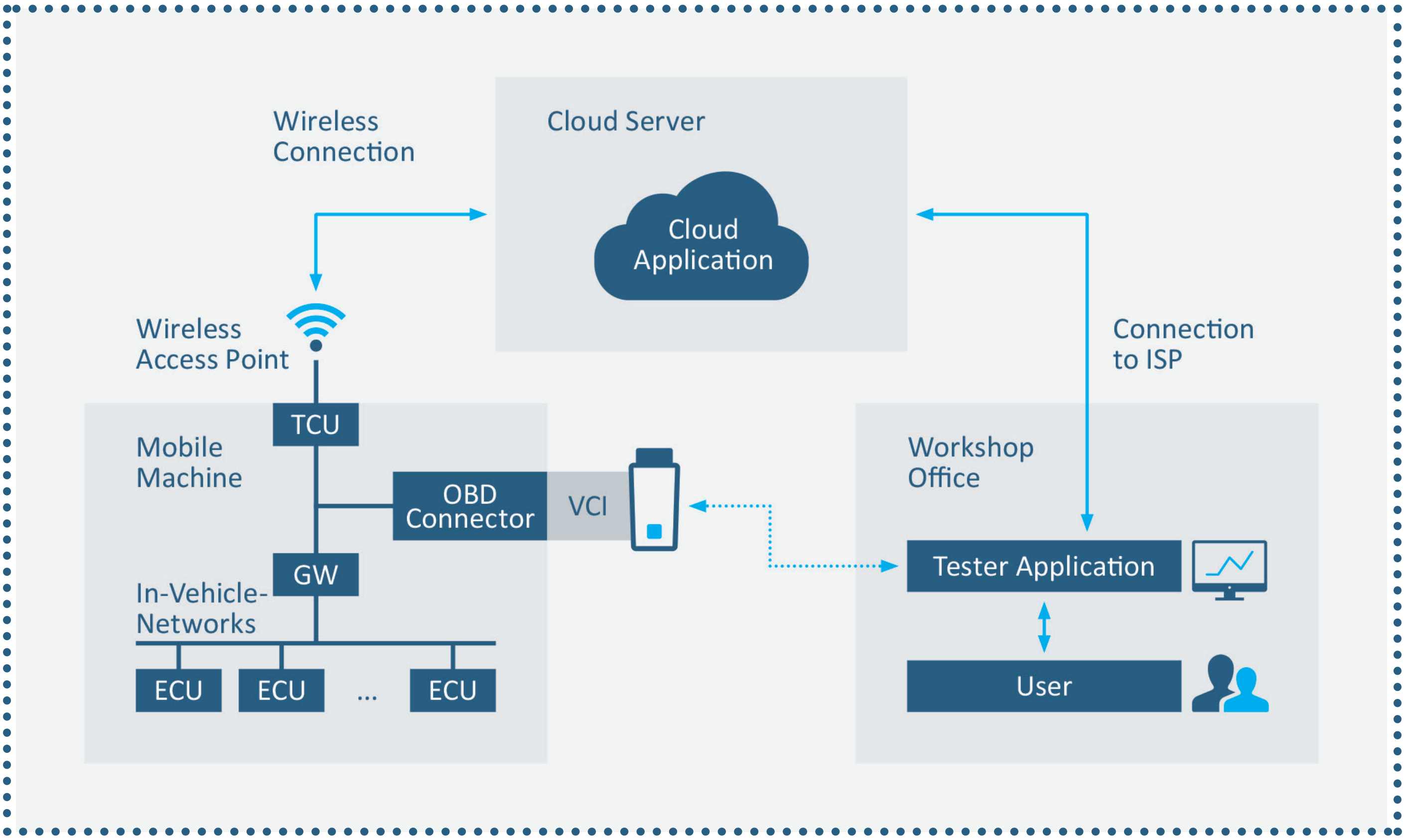

Figure 2: Gateways for Hacker Attacks from the Application to the Vehicle
(© Softing Automotive)

and, if necessary, stores the information in a database.

At first glance, an everyday scenario in a modern automotive environment. If you look more closely though, you will find the first point of attack on the side of the tester application: Does the tester application have sufficient protection against unauthorized access or hacking? Careless dealings with access data, familiar from the office sector, is an enormous risk. But even the best safeguarding of diagnostic software will not help if the relevant rights have been assigned half-heartedly: Is the relevant user actually entitled to run the particular service? Not every user should be able to program or code ECUs. In many cases it is useful to initially limit authorizations to reading services exclusively and to clarify, when the situation arises, if and for how long an extension of those rights is useful.

A further important point is the storage of collected data: Maximum protection of the data against unauthorized access is absolutely imperative! In the era of big data, this data is one of the most important targets for hackers.

The only thing left to mention is the data connection over the Internet: The possible forms of attack are diverse: Virtually everything is conceivable from eavesdropping on communication through manipulating data to taking over the communication link. Avoiding such man-in-the-middle attacks places enormous demands on securing the data connection.

...and How to Close Them

To achieve maximum security, End2End encryption is absolutely necessary whereby this ends at the first interface in the vehicle. A diagnostic system has no influence on the communication within the vehicle. Encryption in this area is the responsibility of the OEM.

A high degree of security can be obtained with suitable access rights, sustainable licensing as well as the use of modern encryption methods on the side of the diagnostic application as well as the data stored. Encryption is also the keyword for ODX and OTX data necessary for diagnostics. Furthermore, it is necessary for suitable processes and tools to prevent access by unauthorized persons.

Symmetrical and asymmetrical encryption methods are possible for safeguarding a data connection. As both procedures have advantages and disadvantages, decisions have to be made on an individual basis as to which procedure should be used. The security level can be increased with additional encryption at protocol level. In the case of UDS, one of the most widely used diagnostic protocols in the automotive environment, this is not possible due to the defined standard; for the newcomer among the diagnostic protocols, ‘DoIP’, TLS encryption is already being prepared as the standard.

In among all these security precautions, however, important aspects for diagnostics, such as for example performance and handling, must not be neglected.

Remote Diagnostics with Softing SDE

The large number of necessary tester applications inevitably requires high performance diagnostic middleware which implements diagnostic methods in a uniform way and which can be integrated simply. One example is Softing SDE (Smart Diagnostic Engine). This combines industry-tested diagnostic components for processing standardized diagnostic data (ODX and OTX – ISO 22901 and ISO 13209) with an easy-to-understand API. This makes the most important diagnostic methods available as functions, for example reading the error memory and programming the ECU. The service-oriented approach pursued is completely remote-capable, unlike the standards it is based on, and the communication links are relatively easy to safeguard using standard mechanisms. Customers implement this to be able to use the same diagnostic functionality in the engineering tester and at the test benches, which nowadays are normally operated at different sites. The advantages of engineering distributed all over the world are thus given a further efficiency criterion.

New Diagnostic Possibilities – For Sure!

In the future, diagnostics and communication in and around the vehicle will play an ever more important role in the automotive sector – whether in engineering, manufacturing, during operation or in the after-sales sector. Paired with these are the constantly increasing demands of security. It is now imperative to balance these two areas ensuring safe operation and the diagnostics of a vehicle in the future too.
This is particularly evident when you think of topics such as autonomous driving.
And this is why it is all the more important that, in the future, solutions are available which, on the one hand, take aspects of security on the basis of the current state of the art into consideration and, on the other, conveniently make the actual functionality available.
Security has to be an integral part of the solution, not an add-on.

>> automotive.softing.com

Markus Steffelbauer heads up Product Management and Marketing at Softing Automotive and is a committed member of standardization bodies.

Günter Fahböck is a Project Manager at Softing Automotive. He specializes in cyber security in the diagnostic environment.

Originally published in German in the section “Measurement - Test - Diagnosis” of the technical magazine
HANSER automotive 10/2019, published by Carl Hanser, Munich, Germany