ACS – Automotive CyberSecurity
Confident in security?
Automotive electronic as attack surface

Almost everyone has read the headlines of cyber security attacks on cars: from odometer manipulation and engine tuning to bypassing the immobilizer or affecting the steering and braking behavior - sometimes even remotely. The reports usually only reflect the special cases that attract a lot of attention. But many other cases and details are being discussed in relevant forums and dedicated conferences – and the trend is increasing.

The number of attacks on automotive electronics is growing due to the larger attack surface:
• Increasing number of electronic components in cars
• Strong interaction of the components inside and outside the car
• Growing complexity of components
• Distributed development – sometimes even without considering security requirements.

The complete system is endangered!

Ultimately, a vulnerability in one component can be enough to jeopardize the security of the entire system. A systematic safeguarding of all relevant components is therefore important and now also required by the specifications for type approval according to UNECE 155. Car manufacturers, the OEMs, cannot handle this task on their own as detailed insights into every relevant component are required.

The ISO 21434 therefore also allows the overall evaluation at the OEM also on the basis of the TIER1 information, who in turn can use the TIER2 information. In this way, necessary information on security can be compiled and evaluated across the entire supply chain.
Both, UNECE 155 and ISO 21434, expect OEMs and suppliers to work systematically when it comes to security. Specifications are not only stated for the products, but also for the processes and people. Only the correct interaction of products, processes and people allows the necessary security to be achieved.

The VDA volume "ACSMS" reflects on this in nine chapters with 21 questions, corresponding minimum requirements and an evaluation scheme. Using these materials, audits of the automotive cyber security management system can be carried out efficiently. For this purpose, the scope in the company will be defined and an adaptation (tailoring) to the company-specific situation is checked.

The topics in the VDA volume "ACSMS" include:

- Cybersecurity Management
- Risk identification, assessment, categorization and treatment
- Consistency check
- Cybersecurity specification, verification, validation and approval
- Update of risk assessments
- Cybersecurity Incident Response
- Reporting to authorities
- Cybersecurity management of contractors.

The VDA volume supports
Experts for ACS-Audits

For Automotive CyberSecurity (ACS) it is not enough just to have introduced the processes, the content of the processes has to be right, so that a culture of security and its awareness is promoted. Therefore, it is important that the audits are accompanied by experts with professional skills in cybersecurity and development processes for the automotive industry. Their judgment plays an important role for the audit result.

The VDA QMC offers the training course "ACS experts for automotive cybersecurity management system audits - Qualification". Following the VDA volume "ACSMS" and ISO 21434, the relevant content is conveyed and amplified in extensive exercises. In small groups, various topics of risk analysis and evaluation of process implementations are practiced using examples.
Outlook

The knowledge that cybersecurity is constantly evolving coupled with the experience gained by implementing the standards will certainly lead to further developments. Adjustments and updates are therefore to be expected and will also be reflected accordingly at the VDA.

The publication of ISO 21434 and the implementation of UNECE 155 not only increase awareness of security in cars (Automotive CyberSecurity), but also require specific action to achieve type approvals. This is also an essential foundation for improved security. The implementation at all involved companies and the interaction along the supply chain will be of high relevance.

Internal and external audits will become increasingly important as proof of compliance with specifications and thereby also the compliance with the relevant standards. Here, the VDA volume "ACSMS" and the training of ACS experts will form the base for the implementation.
Contact

Open Trainings
Phone: +49 30 897842-252 and -253
E-Mail: seminare@vda-qmc.de

Inhouse Trainings
Phone: +49 30 897842-255
E-Mail: inhouse@vda-qmc.de

Live Online Trainings
Phone: +49 30 897842-257
E-Mail: seminare@vda-qmc.de

Training License Partners
Phone: +49 30 897842-254 and -256
E-Mail: licence@vda-qmc.de