Media information

Automotive: asvin offers innovative CSMS update monitoring for the entire software supply chain

Stuttgart, 23.03.2021. The set of regulations developed by the Inland Transport Committee of the UNECE (United Nations Economic Commission for Europe) poses extreme challenges for the automotive industry: If manufacturers and suppliers fail to integrate comprehensive management systems for cybersecurity in vehicles by 2022, the industry faces an estimated loss of one billion euros. Stuttgart-based start-up asvin has developed a modular solution that provides key building blocks for cybersecurity systems. These include documentation and verification of software as well as verification of firmware within the supply chain from the OEM to the vehicle.

To ensure that autonomous driving does not become a nightmare due to hacker attacks, according to UNECE WP 29 (United Nations World Forum for Harmonization of Vehicle Regulations), cybersecurity is to be included as an integral part of type approval from 2022. In addition to establishing a legal framework for OTA updates, the regulations require manufacturers to introduce a cyber security management system (CSMS) in the vehicle. From 2024, the regulation will apply to all new registrations.

Building CSMS on a modular basis

"Despite the long lead time, it is to be feared that vehicle manufacturers will not manage to develop and deploy appropriate all-encompassing systems by next year," explains Dr. Klaus Schaaf, former head of the California Electronics Research Lab and of "Wireless Wolfsburg" at Volkswagen AG and now a consultant for automotive mobility and edge technologies. "Currently, there are no systems that can
both address ever-changing security requirements and ensure compatibility of legacy systems. In order to design fully functional cybersecurity systems, it is important to, both CSMS and SUMS (Software Update Management Systems) to be modular and to generate corresponding system modules that meet the industry standard."

The Stuttgart-based cybersecurity experts at asvin have developed such a module, which makes it possible to track and document the integrity and security status of software throughout the production process and operation on the vehicle. The solution allows, for example, the exact inventory of installed software to be collected for each vehicle and the path of the software from the supplier to the vehicle to be monitored in a process-safe manner. This makes it possible to detect manipulations of the software in the entire process chain, and the software inventory can be compared with known vulnerabilities in risk monitoring for each vehicle. The system from the Stuttgart-based cybersecurity professionals also uses decentralized consensus mechanisms and smart contracts to protect information from manipulation and provide rules in the software supply chain for automations, such as over-the-air updates.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

This provides significant security advantages over solely centralized certificate-based systems. The asvin Chain-of-Trust thus creates the basis of trust for software supply chains from the certification of a software to the update of a device and the operation of the software. In addition, manipulation attempts by attackers can be quickly detected and averted via interfaces in device management and device monitoring.

Security check at every system start

With asvin's solution, manufacturers and suppliers can easily ensure compliance with the most important legal requirements according to UNECE WP 29 and ISO / SAE 21434. Says CEO Mirko Ross: "asvin's service documents every change to software and hardware, as well as data transfer to or from the vehicle, enabling a comprehensive cybersecurity system that focuses on focused on uninterrupted operations. As part of the monitoring process, it is possible to check the system for deviations before each startup." A whitepaper from asvin on "Software and Data Documentation and Regulatory Compliance for the Automotive Industry" is available for free download at asvin.io.

Reprint free of charge, please provide proof (print, scan, link).

About asvin GmbH
Founded in September 2018, Stuttgart-based asvin develops a secure open source solution for the software lifecycle in the Internet of Things. The application enables to close security gaps in the IoT and IIoT and thus to manage business processes without risk. asvin was awarded Best Cybersecurity Start-up in Germany in 2020 on the occasion of it-sa.
Further information: www.asvin.io

Image material
The following images may be used free of charge in the context of reporting on asvin GmbH, provided that the source reference is given.
free of charge in the context of reporting on asvin GmbH, provided that the source reference is given.
High-resolution files are available on request to medien@seidel-kommunikation.de. The photographic material may only be used for editorial reporting on asvin GmbH.

asvin GmbH
Schulze-Delitzsch-Str. 16
70565 Stuttgart
T 0711 2204093 0
F 0711 2240493 44

contact@asvin.io
www.asvin.io

@asvin_io

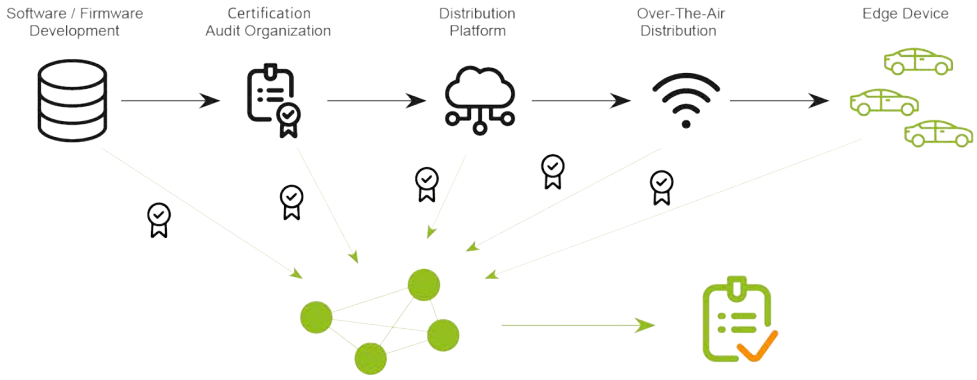
IBAN: DE64 6117 0024 0043 2245 00
BIC: DEUTDEDB611

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart

Image 1/2

The management team of asvin GmbH (from left to right): Mirko Ross (CEO), Sven Rahlfs (COO), Rohit Bohara (CTO) / © asvin GmbH

Image 2/2



Automotive IT security for the entire supply chain
© asvin GmbH

Contact

seidel kommunikation
Agentur für Markenführung und Unternehmenskommunikation
Brunnengasse 3
73650 Winterbach (Stuttgart)
T: 0049 7181 / 26 29 376
E: medien@seidel-kommunikation.de