

Medieninformation

Automotive: asvin bietet innovatives CSMS-Update-Monitoring für die gesamte Software-Lieferkette

Stuttgart, 23.03.2021. Das vom Inland Transport Committee der UNECE (Wirtschaftskommission für Europa der Vereinten Nationen) entwickelte Regelwerk stellt die Automobilindustrie vor extreme Herausforderungen: Schaffen es Hersteller und Zulieferer nicht, bis 2022 umfassende Managementsysteme für Cybersicherheit im Fahrzeug zu integrieren, droht der Branche ein geschätzter Verlust von einer Milliarde Euro. Das Stuttgarter Start-up asvin hat eine modulare Lösung entwickelt, die wichtige Bausteine für Cybersicherheitssysteme zur Verfügung stellt. Dazu gehören Dokumentation und Verifizierung von Software sowie die Überprüfung der Firmware innerhalb der Lieferkette vom OEM bis ins Fahrzeug.

Damit Autonomes Fahren durch Hackerangriffe nicht zum Albtraum wird, soll gemäß des UNECE WP 29 (Weltforum für die Harmonisierung von Fahrzeugvorschriften der Vereinten Nationen) ab 2022 Cybersecurity als integraler Bestandteil in die Typenzulassung aufgenommen werden. Neben der Schaffung eines Rechtsrahmens für OTA-Updates verpflichtet das Regelwerk Hersteller zur Einführung eines Cyber Security Management Systems (CSMS) im Fahrzeug. Ab 2024 greift die Regelung für alle Neuzulassungen.

CSMS modular aufbauen

„Trotz der langen Vorlaufzeit ist zu befürchten, dass es die Fahrzeughersteller bis zum nächsten Jahr nicht schaffen, entsprechende all-umfassende Systeme zu entwickeln und einzusetzen“, erklärt Dr. Klaus Schaaf, ehemaliger Leiter des kalifornischen Electronics Research Lab und von „Wireless Wolfsburg“ der Volkswagen AG und jetzt Berater für Automotive Mobility und Edge-Technologien. „Derzeit gibt es keine Systeme, die sowohl die sich ständig ändernden Sicherheitsanforderungen berücksichtigen als auch die Kompatibilität älterer Systeme gewährleisten. Um voll funktionsfähige Cybersicherheitssysteme zu konzipieren, ist es wichtig, sowohl CSMS als auch SUMS (Software Update Management Systeme) modular aufzubauen und dazu entsprechende Systemmodule zu generieren, die den Industriestandard erfüllen.“

Die Stuttgarter Cybersicherheitsexperten von asvin haben ein solches Modul entwickelt, das es ermöglicht, die Integrität und den Sicherheitsstatus von Software im gesamten Produktionsprozess und Betrieb auf dem Fahrzeug zu verfolgen und zu dokumentieren. Die Lösung erlaubt es beispielsweise, für jedes Fahrzeug den genauen Bestand der installierten Software zu erheben und den Weg der Software vom Lieferanten bis ins Fahrzeug prozesssicher zu überwachen. Damit lassen sich Manipulationen der Software in der gesamten Prozesskette erkennen und der Software-Bestand kann im Risiko-Monitoring für jedes Fahrzeug mit bekannten Schwachstellen abgeglichen werden. Das System der Stuttgarter Cybersicherheitsprofis nutzt zudem dezentralisierte Consensus-Mechanismen und Smart Contracts, um Informationen vor Manipulationen zu schützen und Regeln in der Software-Lieferkette für Automatisierungen, wie beispielsweise für Over-the-Air-Updates, bereitzustellen.



Das bietet deutliche Sicherheitsvorteile gegenüber ausschließlich zentralisierten Zertifikat-basierten Systemen. Die asvin Chain-of-Trust schafft so die Vertrauensbasis für Softwarelieferketten von der Zertifizierung einer Software bis zum Update eines Gerätes und dem Betrieb der Software. Darüber hinaus können über Schnittstellen im Gerätemanagement und Gerätemonitoring Manipulationsversuche durch Angreifer schnell erkannt und abgewehrt werden.

Sicherheitscheck bei jedem Systemstart

Mit der Lösung von asvin können Hersteller und Zulieferer ohne großen Aufwand die Einhaltung der wichtigsten gesetzlichen Bestimmungen gemäß UNECE WP 29 und ISO / SAE 21434 gewährleisten. Dazu CEO Mirko Ross: „Der Service von asvin dokumentiert jede Veränderung an Software und Hardware sowie den Datentransfer zum oder vom Fahrzeug und ermöglicht damit ein umfassendes Cybersicherheitssystem, das sich auf unterbrechungsfreie Betriebsabläufe konzentriert. Im Rahmen des Monitorings ist es möglich, das System vor jedem Start auf Abweichungen zu überprüfen“. Ein Whitepaper von asvin zum Thema „Software and Data Documentation and Regulatory Compliance for the Automotive Industry“ steht unter asvin.io zum kostenfreien Download bereit.

Abdruck honorarfrei, Beleg (Print, Scan, Link) erbeten.

Über die asvin GmbH

Im September 2018 gegründet, entwickelt das Stuttgarter Unternehmen asvin eine sichere Open-Source-Lösung für den Software-Lebenszyklus im Internet der Dinge. Die Applikation ermöglicht, Sicherheitslücken im IoT und IIoT zu schließen und so Geschäftsprozesse ohne Risiko zu bewältigen. asvin wurde 2020 anlässlich der it-sa zum Besten Cybersecurity-Start-up Deutschlands ausgezeichnet.

Weitere Informationen: www.asvin.io

Bildmaterial

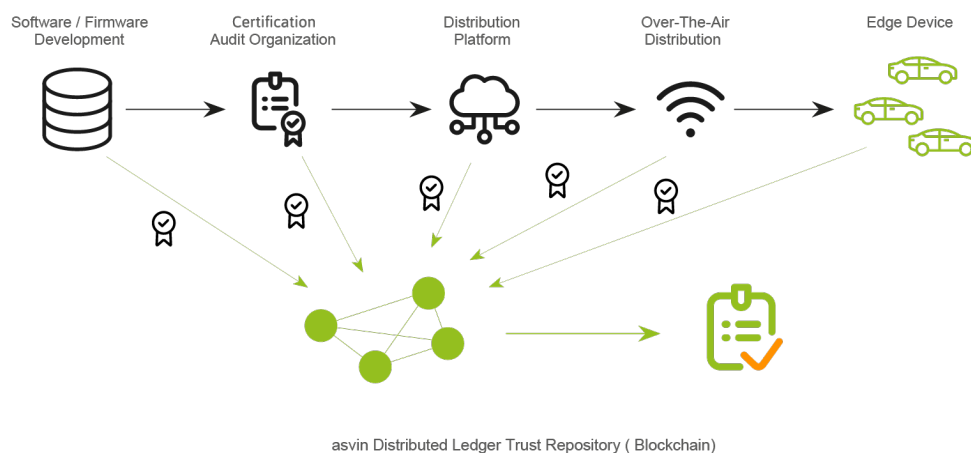
Das nachfolgende Bildmaterial kann im Rahmen der Berichterstattung über die asvin GmbH unter Angabe des Quellenhinweises kostenfrei verwendet werden. Hochaufgelöste Dateien erhalten Sie auf Anfrage an medien@seidel-kommunikation.de. Das Bildmaterial darf ausschließlich für redaktionelle Berichterstattungen über die asvin GmbH eingesetzt werden.

Bild 1/2



Das Führungsteam der asvin GmbH (von links nach rechts): Mirko Ross (CEO), Sven Rahlfs (COO), Rohit Bohara (CTO) / © asvin GmbH

Bild 2/2



Automotive IT-Security für die gesamte Lieferkette
© asvin GmbH

Kontakt

seidel kommunikation
Agentur für Markenführung und Unternehmenskommunikation
Brunnengasse 3
73650 Winterbach (bei Stuttgart)
T: 07181 / 26 29 376
E: medien@seidel-kommunikation.de

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: DEUTDE33HAN33

Sitz Stuttgart
HRB 76700, Amtsgericht Stuttgart