Schutz vor Cyber-Attacken im Automobil

Wie in der Autoindustrie Cybersecurity-Managementsysteme auditiert werden

Ab 2022 müssen Automobilhersteller für die Typzulassung nachweisen, dass sie ihre Fahrzeuge vor Cyberangriffen schützen könnnen und in der Lage sind, Cybersecurity zu managen. Derzeit gibt es mehrere nationale und internationale Aktivitäten zur Standardisierung von Cybersecurity-Managementsystemen und deren Auditierung mit unterschiedlichen Adressanten und Zielsetzungen.

Gunnar Harde

Heutige Fahrzeuge enthalten ca. 200 bis 300 Mio. Zeilen Softwarecode – Tendenz weiter steigend. Zum Vergleich: Eine Boing 787 kommt auf insgesamt 14 Mio. Zeilen, der Linux-Kernel aus dem Jahr 2018 auf 25,4 Mio. Die Automobilindustrie ist inzwischen einer der größten Softwarelieferanten. Doch je größer der Softwareumfang, desto mehr Angriffsmöglichkeiten bieten sich.

Vor fünf Jahren demonstrierten die beiden Security-Wissenschaftler Charlie »»

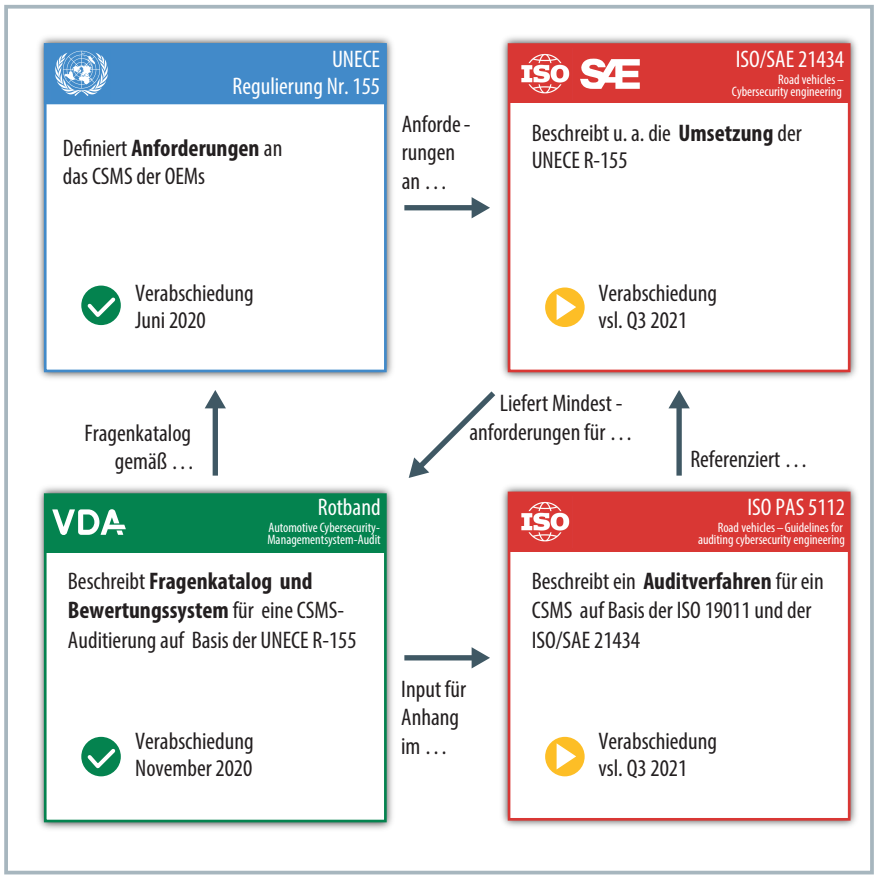

Bild 1. Wer die Herausforderungen von Automotive Cybersecurity verstehen will, muss sich mit verschiedenen Standards und Regeln beschäftigen. Der VDA-Band unterstützt bei Audits. Quelle: VDA © Hnnser

Miller und Chris Valasek, dass ein Jeep Cherokee über das Internet angreifbar ist und ein Angreifer die Kontrolle über Fahrfunktionen übernehmen kann. Ein Jahr später – die kritischen Sicherheitslücken waren bereits geschlossen – zeigten die beiden Wissenschaftler, dass auch bei hohen Fahrgeschwindigkeiten das Fahrverhalten manipulierbar gewesen wäre. Ein Angreifer in New York hätte ein Fahrzeug auf einem Highway in Kalifornien von der Straße abbringen können.

Der Chrysler-Hack zeigt deutlich, dass nicht nur Datenschutz, Betrieb und Finanzen durch Cyberangriffe bedroht sein können, sondern auch die funktionale Sicherheit und damit Leib und Leben von Verkehrsteilnehmern. Spätestens seitdem steht Cybersecurity oben auf der Agenda der Automobilindustrie.

Neue UNECE-Regeln definieren Anforderungen an OEMs

Die Wirtschaftskommission für Europa der Vereinten Nationen (UNECE) hat auf die Cybersecurity-Herausforderungen der Branche reagiert. Im Juni 2020 hat sie mit der *UN-Regulierung 155* für den europäischen und weitere Märkte formuliert, welche Anforderungen Automobilhersteller hinsichtlich Cybersecurity zukünftig erfüllen müssen.

R-155 beschreibt sowohl die Cybersecurity-Anforderungen für die Typgenehmigung als auch die Anforderungen an das *Cybersecurity-Managementsystem (CSMS)* eines Herstellers (OEM). Ein von einer Genehmigungsbehörde bzw. einem technischen Dienst zertifiziertes CSMS wird dann Voraussetzung für eine Typzulassung sein.

Das CSMS muss u. a. Cybersecurity-Risikomanagement, Verifikation der Komponenten und Validierung der Funktionen hinsichtlich Cybersecurity, Cybersecurity-Incident-Response und Cybersecurity-Management gegenüber Vertragspartnern abdecken.

ISO/SAE 21434 adressieren auch Lieferanten

Neben der UNECE befassen sich auch die ISO und die SAE International mit Automotive Cybersecurity. Deren gemeinsamer Standard *ISO/SAE 21434 „Road vehicles – Cybersecurity engineering“* liegt seit Februar 2020 als Draft International Standard (DIS) vor. Der finale Standard wird sich im Gegensatz zur R-155 der UNECE nicht nur an OEMs richten, sondern auch an Lieferanten und sonstige Vertragspartner der Automobilindustrie, die Cybersecurity-relevante Produkte oder Dienstleistungen anbieten. Zudem wird ISO/SAE 21434 sehr viel umfassender sein als R-155, zumal nicht alle Anforderungen des ISO-Standards von der UNECE gefordert werden.

Die inhaltliche Konsistenz mit ISO/SAE 21434 wurde während der Formulierung der R-155 sichergestellt. Dennoch gibt es einen wichtigen Unterschied: Der Entwurf (DIS) der ISO/SAE 21434 bezieht sich auf elektrische und elektronische Systeme von Fahrzeugen einschließlich deren Komponenten und Schnittstellen. R-155 fordert jedoch zudem auch die Berücksichtigung von Backend-Servern, die mit Fahrzeugen im Feld verbunden sind.

Weder ISO/SAE 21434 noch UNECE beschreiben die Auditierung eines CSMS. Der neue Standard ISO/SAE 21434 konkretisiert viele Punkte der R-155 und bietet sich daher zur Ableitung eines konkreten Audit-Fragenkatalogs an. Jedoch liegt der Standard noch nicht final vor. Die Vielzahl der Rückmeldungen zum DIS zeigt, welche große Bedeutung Cybersecurity im Allgemeinen und ISO/SAE 21434 im Besonderen in der Branche haben. Die Rückmeldungen beschleunigen aber nicht den Abstimmungsprozess und damit die finale Veröffentlichung, mit der aktuell eher in der zweites Jahreshälfte 2021 zu rechnen sein wird. Dies führt zu einem zeitlichen Dilemma, denn die Industrie wartet auf verbindliche Vorgaben für die Auditierung ihrer Cybersecurity-Managementsysteme.

Umsetzung der Cybersecurity-Forderungen unter Zeitdruck

Dazu folgende Überlegung: In der Europäischen Union und weiteren UNECE-Märkten sollen R-155 entsprechende Gesetze im Juli 2022 in Kraft treten, in Japan möglicherweise bereits im Januar 2022. Nehmen wir den Juli 2022 als Zieltermin, so sollte ein OEM mit der Auditierung seines CSMS schon Anfang 2022 beginnen. Bleibt somit nur noch ein Jahr, um:

- das CSMS in den einzelnen Unternehmen anzupassen,

- die Vertragspartner in der Lieferkette, die ebenfalls ein funktionsfähiges CSMS nachweisen sollten, zu identifizieren und den Nachweis einzufordern und
- Auditkompetenz im Bereich Automotive Cybersecurity aufzubauen.

Aufgrund dieser Dringlichkeit hat der Verband der Automobilindustrie (VDA) bereits im Herbst 2018 eine Projektgruppe ins Leben gerufen, die einen Vorschlag für eine Auditierung der Automotive Cybersecurity-Managementsysteme im Januar 2021 veröffentlicht hat.

VDA-Band ACSMS-Audit unterstützt in der Praxis

Der von der Projektgruppe erarbeitete *VDA-Band „Automotive Cybersecurity-Managementsystem-Audit"* besteht im Wesentlichen aus einem Bewertungsschema und einem Fragenkatalog für die CSMS-Auditierung. Der Fragenkatalog deckt alle Anforderungen der UNECE R-155 ab, nicht jedoch Anforderungen aus ISO/SAE 21434, die darüber hinausgehen. Die in dem Fragenkatalog spezifizierten Mindestanforderungen stimmen jedoch weitgehend mit den Anforderungen des DIS von ISO/SAE 21434 überein. Aufgrund der noch zu erwartenden Änderungsumfängen bei der ISO/SAE 21434 wurde auf eine Referenzierung bewusst verzichtet und von dem DIS bei Bedarf abgewichen.

Der VDA-Band richtet sich explizit auch an Lieferanten in der gesamten Lieferkette und andere Vertragspartner. Da die UNECE zwar lediglich ein zu zertifizierendes CSMS bei den OEMs fordert, diese aber bei Bedarf die damit verbundenen Anforderungen an die Lieferkette weiterreichen müssen, können eben auch direkte oder indirekte Geschäftspartner von OEMs zum Nachweis eines funktionsfähigen CSMS aufgefordert werden. Dabei besteht die Gefahr, dass Lieferanten für unterschiedliche Kunden unterschiedliche Nachweise erbringen müssen – mit entsprechend großem Aufwand. Die Anwendung des VDA-Bands soll genau dem entgegenwirken.

Bei der Formulierung des VDA-Bands wurden Anforderungen des Kraftfahrzeugbundesamtes (KBA) als eine Behörde, die für die Typzulassung gemäß den UNECE-Anforderungen zuständig ist, mitberücksichtigt. Somit ist zu erwarten, dass die Auditierungen der OEMs durch deutsche technische Dienste und die Auditierungen gemäß dem VDA-Band vergleichbar sein werden.

Gleichwohl handelt es ich bei der VDA-Empfehlung um einen nationalen Vorschlag aus der Industrie, nicht um einen internationalen Standard. Dieser internationale Standard entsteht derzeit mit *ISO PAS 5112*.

ISO PAS 5112 schließt die Lücke

Da die ISO/SAE 21434 kein Auditverfahren für das CSMS vorgibt, wurde *ISO PAS 5112 „Road vehicles – Guidelines for auditing cybersecurity engineering"* initiiert, um diese Lücke zu schließen.

ISO PAS 5112 wird derzeit formuliert. Mit einer Veröffentlichung ist im Lauf des Jahres 2021 zu rechnen. Es zeichnet sich jedoch ab, dass dieser Standard die *ISO 19011 „Guidelines for auditing management systems"* für den in ISO/SAE 21434 beschriebenen Kontext konkretisieren wird. Im Gegensatz zum VDA-Band steht dort der Auditierungsprozess im Vordergrund. Ein Fragenkatalog für die Auditierung ist (Stand heute) lediglich im informativen Anhang exemplarisch enthalten. Dieser Fragenkatalog entspricht in weiten Teilen dem des VDA-Bands.

Das Gesamtbild besteht aus vier Teilen

Derzeit scheinen sich die verschiedenen Puzzleteile wie folgt zusammenzusetzen:

- UNECE gibt mit R-155 die Anforderungen vor,
- ISO/SAE 21434 wird diese Anforderungen konkretisieren und deren Umsetzung beschreiben,
- der VDA-Band spezifiziert den Fragenkatalog und das Bewertungsschema und
- ISO PAS 5112 beschreibt den CSMS-Auditierungsprozess.

Ob sich dieses Bild verfestigt, wird sich zeigen (Bild 1). Die Kompatibilität zwischen VDA-Band und ISO PAS 5112 wird in der deutschen Spiegelgruppe zu ISO PAS 5112 weiter beobachtet werden. Durch die Veröffentlichung des VDA-Bands ist jedoch eine Vorbereitung auf das CSMS-Audit in den einzelnen Unternehmen bereits jetzt möglich. Sollte es seitens der ISO oder der Genehmigungsbehörden nicht doch noch zu großen Änderungen hinsichtlich der Auditierung kommen, so werden die Vorschläge aus dem VDA-Band auch nachhaltig gültig und anwendbar sein.

Der VDA plant ab diesem Jahr Schulungen zum *Automotive Cybersecurity-Experten* anzubieten. Automotive Cybersecurity-Experten sollen dann Cybersecurity-Managementsysteme (mit) auditieren können.

An Integration der Managementsysteme wird geforscht

Mit dem Automotive CSMS erweitert sich die Familie der Managementsysteme in der Automobilindustrie um ein weiteres Mitglied. Ein Mitglied, das auch für bislang branchenfremde Unternehmen wie die Telekommunikationsbranche relevant sein dürfte. Zudem wird mit dem *Softwareupdate-Managementsystem (SUMS)* noch ein weiteres Managementsystem hinzukommen.

Offen bleibt die Frage, ob die etablierte Managementsystem-Landschaft in der Automobilindustrie diesen neuen Anforderungen zukünftig noch gerecht werden kann oder neue Wege zu beschreiten sind. Das *Automotive Quality Institute* wird dies mit der TU Berlin im Auftrag des VDA in 2021 näher untersuchen. ■

INFORMATION & SERVICE

LITERATUR

- **UNECE:** Proposal for a new UN Regulation on uniform provisions concerning the approval of vehicles with regards to cyber security and cyber security management system, 23.06.2020
- **ISO/SAE:** Road vehicles – Cybersecurity engineering, 21434:2019(X), DIS stage
- **VDA:** Automotive Cybersecurity-Managementsystem-Audit. 1. Auflage, Dezember 2020

AUTOR

Gunnar Harde ist Senior-Projektleiter bei der Automotive Quality Institute GmbH. Er hat bei der Formulierung des VDA-Bands „Automotive Cybersecurity-Managementsystem-Audit" mitgewirkt.

KONTAKT

Gunnar Harde
gunnar.harde@aqigmbh.de