QZ Qualität und Zuverlässigkeit 67. Jahrgang 12/2022

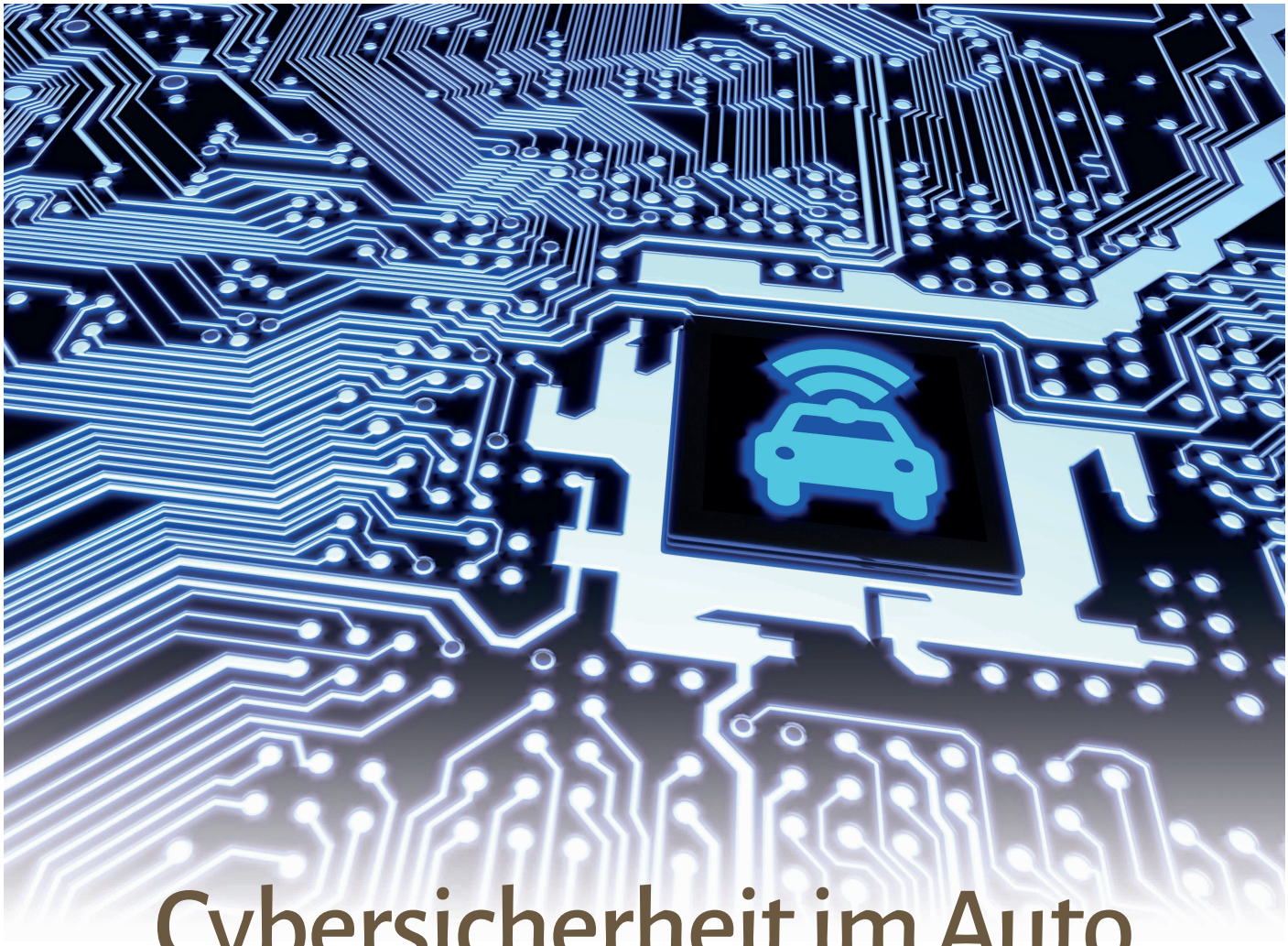
QZ Qualität und Zuverlässigkeit

Die Zeitschrift für Qualitätsmanagement und Qualitätssicherung

www.qz-online.de 12 / 2022

Herausgeber: Deutsche Gesellschaft für Qualität e. V.

HANSER



Cybersicherheit im Auto bleibt eine Herausforderung

Wie ISO/SAE 21434 zur Automotive Cyber Security beitragen soll

Jede zusätzliche Kommunikationsschnittstelle und Komponente, die Autohersteller in ihre zunehmend smarten Fahrzeuge integrieren, ist ein potenzieller Angriffspunkt für Cyberkriminelle. Das Schadenspotenzial einer Manipulation steigt rasant, etwa mit Blick auf autonom gesteuerte Fahrzeuge oder elektronisch gesteuerte Fahr- und Bremsfunktionen. Wie also können Hersteller und Zulieferer mit ISO/SAE 21434 die Weichen für eine systematische und strategische Automotive Cyber Security stellen? Und wo stößt die neue Norm noch an ihre Grenzen?

Holger Schmeken

Die Automobilbranche durchläuft aktuell einen radikalen Paradigmenwechsel: Mit der rasant voranschreitenden Digitalisierung halten immer mehr elektronische Steuersysteme, intelligente Komponenten, Embedded Systems und API-Schnittstellen in Fahrzeugen Einzug – und machen sie leistungsfähiger, sicherer und smarter als je zuvor. Gleichzeitig steigt die Gefahr einer Manipulation von außen. Dazu ein Beispiel aus dem Jahr 2015: Die amerikanischen Sicherheitsforscher Charlie Miller und Chris Valasek luden den Journalisten Andy Greenberg ein, um an einem Jeep Cherokee zu demonstrieren, »»

wie umfangreich der Zugriff durch Hacker auf moderne Fahrzeugsysteme sein kann. Sie kompromittierten das Uconnect-System, das von Infotainment bis Navigation viele elektronische Fahrzeugfunktionen vereint und eine IP-Adresse besitzt. Schlussendlich musste der Journalist machtlos dabei zusehen, wie die IT-Fachleute aus mehreren Meilen Entfernung das gesamte Fahrzeug manipulieren konnten, vom Radio, über die Scheibenwischanlage bis zur Lenkung und Bremse. Die Folge dieses Live Hacks waren ein Rückruf von 1,4 Millionen Fahrzeugen und eine Strafzahlung in Höhe von 105 Millionen Dollar – von den Reputationsschäden und Personenschäden in einem realen Szenario ganz zu schweigen.

Der zunehmende Elektronikeinsatz birgt also Gefahren, denen dringend begegnet werden muss. Im Augenblick ruhen die Hoffnungen der Hersteller auf der ISO/SAE 21434, die seit Juli 2022 für neue Fahrzeugtypen, ab 2024 sogar für alle neu produzierten Fahrzeuge verpflichtend ist und wird. Die Norm soll eine sichere Prüfgrundlage für die konsistente Sicherheit über den gesamten Lifecycle eines Fahrzeugs garantieren. Doch wird sie den hohen Erwartungen auch tatsächlich gerecht?

ISO/SAE 21434 - strategischer Ansatz für mehr Cyber Security

Angesichts immer neuer realer und möglicher Bedrohungsszenarien ist es überdeutlich, dass die Automotive Cyber Security klarer und verbindlicher Leitplanken bedarf. Den grundsätzlichen Rahmen dafür haben die Vereinten Nationen mit zwei neuen Regelungen abgesteckt: der *UNECE Cyber Security (UN R 155)* – deren Umsetzung die neue Norm *ISO/SAE 21434* konkretisiert – und der *UNECE Software-Aktualisierung (UN R 156)*, für deren Umsetzung die Norm *ISO 24089* erstellt wurde.

Hinter der ISO/SAE 21434 steht die Idee, die eher allgemein gehaltenen Anforderungen aus UN R 155 mit konkreten Handlungsanweisungen für die Umsetzung zu unterstützen und so die Cyber-Sicherheit gemäß des Security-by-Design-Ansatzes konsistent in alle Bereiche des Automobilbaus bis hin zu den Lieferanten zu integrieren. Denn in einer Sache sind sich Experten für Informationssicherheit einig: Punktuelle Maßnahmen reichen nicht mehr aus, um die aus vielen softwaregesteuerten Komponenten bestehenden Fahrzeuge ganzheitlich zu schützen. Stattdessen bedarf es neuer systematischer und strategischer Ansätze, die klare Anforderungen an den Umfang, die Leistung und die Auditierung eines Security-Systems vorgeben und den gesamten Produktlebenszyklus abdecken: von der Konzeption bis zur Stilllegung eines Fahrzeugs. Dafür gilt es, den Blick vor allem auch auf die langfristige Verfügbarkeit und auf die Einbindung der gesamten Supply Chain zu richten.

Mit Cyber Security Management gegen digitale Gefahren

Um diesem ganzheitlichen Sicherheitsansatz gerecht zu werden, definiert ISO/SAE 21434 ein *Cyber Security Management System (CSMS)*, das die Bereiche Sicherheitskonzeption, Produktentwicklung, Produktwartung, Risikoerkennung, Gefahrenabwehr, Produktentsorgung und alle relevanten fortlaufenden Prozesse integriert. Darüber hinaus definiert die Norm Regelungen für die Verantwortlichkeiten bei einer verteilten Produktentwicklung zwischen Hersteller und Lieferanten.

Schon beim ersten Blick in die neue Norm zeigt sich, dass diese deutlich umfassender als die UN R 155 ist und tatsächlich alle wesentlichen Aspekte und Anforderungen einschließt. Für OEMs und Zulieferer bietet eine Auditierung nach ISO/SAE 21434 also in vielen Bereichen einen hohen Mehrwert – Stichwort: Cyber-Versicherung, Cyber-Haftung, Lieferantenbewertung und natürlich Marktreputation. Auf diese Weise kann sie sogar zum echten Wettbewerbsvorteil werden. Immerhin gilt von unabhängigen Experten bestätigte IT-Sicherheit und bestätigter Datenschutz zunehmend als wichtiges Qualitätsmerkmal.

Fehlende Audit-Sicherheit ist aktuell eine Manko

Die Vorzüge einer Auditierung gemäß SAE/ISO 21434 sind unbestritten, doch dafür benötigt es einer robusten Prüfgrundlage, die lückenlose Sicherheit und Vergleichbarkeit bietet. Und genau an diesem Punkt weist ISO/SAE 21434 aus Sicht vieler OEMs noch relevante Schwächen auf.

Zwar enthält die Norm weitreichende Regelungen für alle Bereiche der Cyber Security. Sie äußert sich aber nicht zu spezifischen Technologien oder Lösungen, was für Hersteller und Lieferanten eine wertvolle Hilfestellung wäre. Und, noch gravierender: Es gibt für Auditoren derzeit noch keinen verbindlichen Prüfkatalog, wodurch die Sicherheit der Prüfgrundlage fehlt. Darunter leidet aus Sicht der OEMs die Vergleichbarkeit zwischen Audits verschiedener Prüfdienstleister – etwa, welche Standorte eines Lieferanten in die Prüfung einbezogen werden oder welche Vertragszusagen des Lieferanten gegenüber dem OEM zur Steuerung des Prüfungsablaufs herangezogen werden. In der komplex und dezentral organisierten Automotive-Branche ist dies ein gravierendes Problem, das den Start und den Erfolg des relativ jungen Standards massiv erschweren könnte.

Cyber Security wird zum Qualitätsmerkmal

Doch es gibt gleich mehrere Silberstreife am Horizont: Der Verband der Automobilindustrie (VDA) hat schon vor einiger Zeit mit dem VDA-Band *Automotive Cybersecurity Management System Audit (ACSMS)* einen hilfreichen ersten Fragebogen inklusive konkreter Bewertungskriterien veröffentlicht, um OEMs und Zulieferer bei der erfolgreichen CSMS-Auditierung zu unterstützen. Die Veröffentlichung war zu dieser Zeit eine Reaktion auf das nahende Inkrafttreten von ISO 21434. Auch wenn es damals noch keine klare Grundlage für die Prüfprozesse gab, hilft der VDA-Band Unternehmen in vielen Bereichen, sich auf ein mögliches Audit vorzubereiten.

Darüber hinaus lieferte die Ausarbeitung durch den VDA als nationaler Verband eine hervorragende Grundlage für den internationalen Standard *ISO PAS 5112 Road Vehicles – Guidelines for Auditing Cybersecurity Engineering*, der im März 2022 ver-

INFORMATION & SERVICE

AUTOR

Holger Schmeken ist Programm Manager und Information Security Officer der DQS Bit GmbH, dem DQS Center of Excellence für ISMS und TISAX. Der Experte für Informationssicherheit und Softwareentwicklung bringt seine Expertise zudem als Auditor für ISO 27001 mit KRITIS-Prüfverfahrenskompetenz ein.

KONTAKT

Holger Schmeken
holger.schmeken@dqs.de

öffentlicht wurde. Diese Norm sollte explizit die Lücken im Prüfkatalog schließen und die Weichen für eine verbindliche Auditierung von ISO/SAE 21434 stellen. Und selbst wenn einige OEMs beklagen, der im Anhang enthaltene Prüfkatalog sei nicht konkret genug und biete nicht den erforderlichen Umfang, adressiert die Norm doch eine ganze Reihe offener Fragen – und sollte für Auditverantwortliche eine Pflichtlektüre sein.

Auch weitere nationale und internationale Automotive-Verbände haben signalisiert, dass sie derzeit mit Hochdruck – und häufig in enger Kooperation mit führenden OEMs – an der Ausarbeitung einer besseren Prüfgrundlage arbeiten. Der Stand dieser Entwicklung befindet sich bereits in der Phase erster Testaudits – es ist also zu erwarten, dass sich in diesem Bereich in naher Zukunft noch viel tun wird, was ISO/SAE 21434 als willkommene Starthilfe dienen dürfte.

Fazit: Holistische Cyber Security-Ansätze werden in der Automobilbranche immer wichtiger und zu einem entscheidenden Qualitätsmerkmal. Dabei sind die Anforderungen wesentlich höher als im Telekommunikationsbereich, in dem die Garantien für Software-Updates teilweise nur wenige Jahre betragen. Doch ein kompromittiertes, angegriffenes Auto ist für den Hersteller wie auch den Konsumenten ein wesentlich höherer Risikofaktor.

Die Branche hat dies längst erkannt und arbeitet auf allen Ebenen und über alle Institutionen daran, die elektrischen und elektronischen Systeme über die gesamte Wertschöpfungskette und den vollständigen Lifecycle abzusichern. Erste Regelungen und Standards sind bereits in Kraft getreten und teilweise verpflichtend. Dennoch gilt es, die Operationalisierbarkeit der Normen weiter zu verbessern, um nicht nur die Cyber-Sicherheit der Fahrzeuge, sondern auch die Sicherheit der Prüfgrundlage konsistenter zu gestalten. ■

Automotive Cyber Security

Wen betreffen die neuen Regelungen?

In den beiden neuen *UN-Verordnungen UN R 155 und UN R 156* ist vor allem von den Fahrzeugherstellern die Rede, die zur Umsetzung der neuen Anforderungen verpflichtet sind. Dazu gehört es allerdings auch, die Cyber-Sicherheit über die gesamte Lieferkette hinweg zu beobachten und zu überprüfen, um die Durchsetzung der Regelungen jederzeit nachweisen zu können. Der Hersteller ist also zur Kontrolle der Zulieferer verpflichtet. Und er wird seine Lieferanten daher mit hoher Wahrscheinlichkeit ebenfalls zur Umsetzung der neuen Standards verpflichten.

Die beiden Verordnungen gelten für PKW, Kleintransporter, LKW und Busse, sofern diese mit automatisierten Fahrfunktionen ausgestattet sind. In diese Kategorie entfallen auch neuartige automatisierte Pods, Shuttles oder vergleichbare Vehikel. Darüber hinaus gelten die Regelungen auch für Anhänger, die mindestens ein elektronisches Steuergerät enthalten.

Was sind wesentliche Merkmale eines Cyber Security Management Systems (CSMS)?

- Risikomanagement: Ein Unternehmen nutzt Prozesse zur Risikoerkennung, Risikobewertung und Risikominderung von Cyber-Gefahren
- Das Risikomanagement deckt den gesamten Produktlebenszyklus ab – von der Entwicklung über die Betriebsphase bis zur Stilllegung
- Monitoring von neuen Schwachstellen und bekannten Angriffen, um mit neuen Updates reagieren zu können.
- Ermöglicht ein unabhängiges Assessment durch ein akkreditiertes Prüfinstitut.