Ohne Cybersecurity fährt künftig nichts mehr

Cybersicherheit wird zur Compliance-Herausforderung für die Autoindustrie

Mit der ISO/SAE 21434 entsteht ein zentraler Dreh- und Angelpunkt für Cybersicherheit in der gesamten Automotive-Wertschöpfung. Mit der Spezifikation ISO/PAS 5112 wird das zugehörige Audit greifbar. Die Compliance mit den Forderungen dieses Standards betrifft OEMs ebenso wie deren Lieferanten.

Philipp Veronesi und Manuel Sandler

Was derzeit die gesamte Automobilwertschöpfungskette weltweit beschäftigt ist ein Veränderungsprozess, wie er in der über hundertjährigen Geschichte des Autos einmalig ist: Die digitale Transformation erreicht das Auto. Und das gesamte zugehörige Ökosystem gleich mit. Und zwar rasend schnell. Von 0 auf 100 erst in den letzten Jahren.

Während Google, Amazon, Facebook & Co ihr Kerngeschäft mit Milliarden Nutzern über Jahre noch ziemlich ungestört ausbauen konnten und die Gesetzgebung nur schleppend hinterherkommt, zugehörige Regularien festzulegen (z. B. EU-DSGVO), stellt sich für die Automobilindustrie die Ausgangslage heute völlig anders dar. Auch deshalb, weil etwa mit dem UNECE World Forum for Harmonizations of Vehicle Regulations (UNECE WP.29) seit fast 70 Jahren bereits einheitliche Regelungen für den Fahrzeugbau erarbeitet werden. Konkrete spezifizierte Sicherheitsvorschriften für die gesamte Automobilzulieferindustrie sind daher eher die Regel als die Ausnahme.

Entsprechend klar, dass nun auch für den Cyberspace rund um das Automobil konkrete Standards und Regularien erforderlich werden. Auch die Autoindustrie stellte Forderungen, in dieser neuen Dimension der Wertschöpfung zeitnah für Verbindlichkeit zu sorgen.

ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering

Mit *SAE J3061 Cybersecurity Guidebook for Cyber-Physical Vehicle Systems* wurde Anfang 2016 durch die Society of Automotive Engineers (SAE) der erste Versuch unternommen, verbindliche Guidelines für Cybersicherheit zu etablieren.

Abgelöst werden diese Guidelines durch *ISO/SAE 21434 Road Vehicles – Cybersecurity Engineering*, für die sich die SAE mit der International Organisation for Standardization (ISO) erstmals zusammengeschlossen hat, um einen neuen Automobil-Industriestandard zu definieren. ISO/SAE 21434 soll für den gesamten Produktlebenszyklus einen Rahmen definieren, was in Bezug auf die Gewährleistung von vollumfänglicher Cybersicherheit an welcher Stelle (und wie) zu tun ist.

Aktuell (August 2021) warten wir noch auf die finale Variante des Standards ISO/SAE 21434, die für Ende 2020 geplant war. Dennoch sind die Entwürfe (Drafts), ISO/SAE DIS 21434 (Draft International Standard, DIS) sowie die neuere ISO/SAE FDIS 21434 (Final Draft International Standard, FDIS) bereits öffentlich zugänglich. Die intensive Auseinandersetzung mit den Themen, die der Standard beschreibt und verlangt, hat bereits begonnen.

Sprechen wir nun einfach über ein paar neue Anforderungen an das Produkt, die es zu erfüllen gilt? Weit gefehlt! Experten sind sich einig: ISO/SAE 21434 betrifft auf nie erlebte Weise die Gesamtorganisation, Entwicklungsprojekte, Engineering-Prozesse sowie alle beteiligten Rollen und Abläufe. Denn wenn Cybersicherheit ganzheitlich gewährleistet werden soll, ist die Kette immer nur so stark wie ihr schwächstes Glied. Vom Entwicklungsingenieur bis zum Lagerarbeiter über den Verkäufer bis zum Werkstattmitarbeiter und darüber hinaus: Cybersicherheit im Automobil wird ein Thema für alle Beteiligten.

ISO/SAE 21434 fordert nicht nur die Original Equipment Manufacturer (Autohersteller, OEM) – alle Zulieferer elektrisch-elektronischer Systeme (E/E Systeme) entlang der gesamtem Wertschöpfungskette sind angehalten, dem Standard zu folgen. Dabei ist klar, worum es im Kern geht: Produktsicherheit gewährleisten, den Fahrer und die Umgebung bestmöglich schützen. Auch für den Schadenfall muss es einen Argumentationsrahmen geben, mit dem sich nachweisen lässt, dass auch im komplexen Bereich der Gewährleistung von Cybersicherheit State-of-the-Art gearbeitet wurde.

Vereinfacht kann man es so erklären: Sollte einmal etwas Unvorhergesehenes passieren und es kommt, aus welchen Gründen auch immer, zu einer Verhandlung des Falls vor Gericht, so ließe sich die

korrekte Anwendung des Standards ISO/SAE 21434 heranziehen. Man könnte nachweisen, ob Abläufe, Prozesse und Arbeitsergebnisse korrekt im Rahmen des aktuellen Industriestandards gehandhabt wurden.

ISO/SAE 21434 verpflichtend für die gesamte Lieferkette

In der Praxis lässt sich derweil Folgendes beobachten: OEMs, die mit ISO/SAE 21434 in die Pflicht genommen werden, die Anwendung des Standards entlang der gesamten Lieferkette sicherzustellen, geben diese Bürde nun einfach weiter. Sie fordern pauschal die Anwendung dieses Standards von ihren Zulieferern.

Dadurch entsteht im ungünstigsten Fall die von Experten gefürchtete Situtation „Cybersecurity als Add-On". Frei nach dem Motto, dass die Lieferantenauswahl und die Verhandlung der Geschäftsbeziehungen, sowie die Zusammenarbeiten an Entwicklungsprojekten bereits voran getrieben werden, und es dann heißt, bitte auch noch Cybersicherheit integrieren – das steht hier auch noch auf der Liste.

Die entsprechenden Abstimmungsnotwendigkeiten rund um Cybersicherheit zwischen OEMs und den Tier-x-Zulieferern entlang der laufenden und zukünftigen Entwicklungsprojekte nehmen folglich bisher ungeahnte Ausmaße an. Dass diese derzeit auf der ganzen Welt noch immer Pandemie-bedingt remote und aus dem Home Office stattfinden, ist dabei nicht die größte Herausforderung.

Wie steht es aktuell um das Audit zur ISO/SAE 21434?

Entsprechend wird in der Industrie – neben dem reinen Verstehen und Anwenden des ISO/SAE 21434 Standards – insbesondere die Frage nach dem zugehörigen Audit zum Thema. Die korrekte Anwendung der Prinzipien von ISO/SAE 21434 in der Praxis ist das eine. Der für Lieferantenverhandlungen möglicherweise weitaus relevantere Punkt ist die zugehörige Dokumentation der Compliance mit ISO/SAE 21434.

Wie kann die durchgehende Konformität zur ISO/SAE 21434 also bestätigt werden?

Genau an dieser Stelle kommt *ISO PAS 5112 Road Vehicles – Guidelines for auditing cybersecurity engineering* ins Spiel. Diese Spezifikation wird wichtig, wenn es um die zukünftige Auditierung gemäß ISO/SAE 21434 geht. Ziel der ISO PAS 5112 ist es, Organisationen bei der Auditierung der erreichten Cybersicherheit (in der eigenen Organisation und entlang der Lieferkette) zu unterstützen.

Derzeit liegt ISO PAS 5112 noch in der Comittee-Draft-Version vor. Die Spezifikation befindet sich also noch weiter in der Entwicklung durch das zugehörige ISO-Arbeitsgremium.

ISO PAS 5112 liefert zunächst Richtlinien für das allgemeine Management eines Auditprogramms. Dann geht es weiter mit konkreten Inputs für die Planung und Durchführung des eigentlichen Audits. Und zu guter Letzt werden die Anforderungen an den Auditor und seine Evaluationsarbeit spezifiziert.

Auch ISO PAS 5112 setzt einen Schwerpunkt bei der Prüfung, ob ein Cybersecurity Management System (CSMS) erfolgreich etabliert wurde. Hier fordert etwa die *UN Regulation No. 155 – Cyber security and cyber security management system (UN R155)*, dass OEMs verpflichtet werden, die Anwendung eines CSMS nachzuweisen. Dies ist sogar eine Vorrausetzung für Typgenehmigungen. Zu beachten ist hierbei, dass die UN R155 explizit das Management der Risiken entlang der gesamten Lieferkette beschriebt. So gilt für den OEM, dass er dies auch entlang der gesamten Wertschöpfungskette über alle Vertragspartner hinweg, sicherstellt.

Wird es ein Zertifikat für ISO/SAE 21434-Compliance geben?

Unabhängig von der Durchführung eines Audits, als „Momentaufnahme" stellt sich derweil insbesondere auf Seiten der Zulieferer die Frage, ob es auch ein ISO/SAE 21434 Zertifikat geben wird. Etwas, das man als Siegel an die Abteilung oder die gesamte Organisation hängen kann und bestätigt „Hier ist alles ISO/SAE 21434-zerfiziert."

Für OEMs wäre dies möglicherweise interessant, denn schließlich wäre dieses Zertifikat ein wichtiges Kriterium bei der Lieferantenevaluation. Die Notwendigkeit, in Bezug auf Cybersicherheit eigene Audits durchführen zu müssen, könnte entfallen. Wenigstens könnte der Aufwand dafür deutlich reduziert werden.Mit dem TISAX-Zertifikat gibt es in der Automobilindustrie bereits einen ähnlichen Ansatz im Bereich der Informationssicherheit. Derzeit (August 2021) ist die Frage nach einem ISO/SAE 21434-Zertifikat noch nicht abschließend geklärt.

Ziehen wir hier den Vergleich zum Certificate of Compliance for CSMS, also dem Zertifikat zur korrekten Etablierung eines CSMS, wie es die UN R155 vorsieht, dann wird klar: Die Rechte der Zulassungsbehörde, (etwa das Zertifikat wieder zu entziehen, sollten beteiligte Prozesse nicht mehr hinreichend erfüllt sein) und die Pflichten der OEMs (z. B. Meldungen abzugeben, sollten sich Aspekte geändert haben, die eine neue Prüfung erforderlich machen könnten) sind weitreichend.

Fazit: Wenngleich die „offizielle Handhabe„ mit Blick auf die Auditierung und Zertifizierung rund um die Standards und Regularien der Cybersicherheit im Automobilkontext noch nicht abschließend geklärt ist – Fest steht, dass da etwas kommen wird. Mit Blick auf die enge Zeitachse bis zur effektiven Anwendung, empfehlen Experten bereits im Vorfeld frühzeitig die Berücksichtigung von regelkonformer Cybersicherheit in der Organisation, entlang der Prozesse und darüber hinaus vorab auf den Prüfstand zu stellen. ■

INFORMATION & SERVICE

LITERATUR

The Essential Guide to ISO/SAE 21434
www.cyres-consulting.com/book

AUTOREN

Philipp Veronesi ist Gründer und Geschäftsführer von Cyres Consulting. Neben langjähriger praktischer Erfahrung im Engineering verantwortete er auch das Management technisch anspruchsvoller Entwicklungsprojekte für führende Unternehmen der Automobilindustrie.

Manuel Sandler ist Associate Partner bei Cyres Consulting. Er verfügt über vielseitige Erfahrung im globalen Projekt- und Prozessmanagement der Automotive-Wertschöpfungskette, einschließlich OEMs und Tier-1. Er ist ASPICE Provisional Assessor und Experte für Engineering Process Development, ISO 26262, ISO/IEC 15288 und die ISO/SAE 21434.

KONTAKT

Arne-P. Berg
T 089 9542808-00
office@cyres-consulting.com