VDA QMC

Verband der Automobilindustrie
Qualitäts-Management-Center

ACS – Automotive CyberSecurity

Alles sicher?



Herausgeber

VDA QMC

Qualitäts-Management-Center im
Verband der Automobilindustrie e.V.
Behrenstraße 35, 10117 Berlin
www.vda-qmc.de

Automobil-Elektronik als Angriffsfläche

Fast jeder hat schon mal die Headlines von Cyber-Security-Angriffen auf Autos gelesen: von Tachomanipulationen und Motor-Tuning über das Überlisten der Wegfahrsperre bis hin zum Eingriff in Lenkung und Bremsverhalten – teilweise sogar aus der Ferne. Dabei spiegeln die Berichte meist nur die besonderen Fälle wider, welche viel Aufmerksamkeit erregen.
In einschlägigen Foren und Fachkonferenzen werden viele weitere Fälle und Details diskutiert – mit steigender Tendenz.

Die Anzahl der Angriffe auf die Automobil-Elektronik wächst aufgrund der größeren Angriffsfläche:

- Zunehmende Anzahl von elektronischen Komponenten im Auto
- Starke Vernetzung der Komponenten im und außerhalb des Autos
- Wachsende Komplexität der Komponenten
- Verteilte Entwicklung – teilweise ohne Berücksichtigung der Sicherheitsanforderungen.

Das komplette System ist gefährdet!

Letztlich kann eine Schwachstelle in einer Komponente ausreichen, um die Sicherheit des kompletten Systems zu gefährden. Eine systematische Absicherung aller relevanten Komponenten ist daher wichtig und wird nunmehr durch die Vorgaben zur Typenzulassung nach UNECE 155 gefordert. Dabei kann der OEM als Autohersteller allein diese Aufgabe nicht bewältigen, braucht es doch die Detail-Einsicht in jede relevante Komponente.

Die ISO 21434 erlaubt daher die Gesamtbewertung beim OEM auch auf Basis der TIER1-Informationen, welche sich wiederum der TIER2-Information bedienen können. Somit können über die gesamte Lieferkette die Sicherheitsinformationen zusammengetragen und bewertet werden.





Der Band gibt Hilfestellung

Sowohl die UNECE 155 als auch die ISO 21434 erwarten ein systematisches Arbeiten in Punkto Sicherheit bei den OEMs und Zulieferern. Dabei sind Vorgaben nicht nur für die Produkte, sondern insbesondere auch für die Prozesse und Personen definiert. Denn letztlich erlaubt nur das korrekte Zusammenspiel von Produkten, Prozessen und Personen das Erreichen der nötigen Sicherheit.

Der VDA-Band „ACSMS“ reflektiert dies in neun Kapiteln mit 21 Fragestellungen, entsprechenden Mindestanforderungen sowie einem Bewertungsschema. Anhand dieser Materialien können Audits zum Automotive Cyber-Security Management-System effizient durchgeführt werden. Dazu wird der Geltungs- und Anwendungsbereich in der Firma definiert und eine Anpassung (Tailoring) auf die firmenspezifische Situation geprüft.

Die Themenbereiche im VDA-Band „ACSMS“ umfassen:

- Cybersecurity-Management
- Risikoidentifizierung, -bewertung, -kategorisierung und -behandlung
- Konsistenzprüfung
- Cybersecurity-Spezifizierung, -Verifizierung, -Validierung und -Freigabe
- Aktualisierung der Risikobewertungen
- Cybersecurity-Incident-Response
- Berichtswesen gegenüber Behörden
- Cybersecurity-Management der Vertragspartner.

Experten für ACS-Audits

Für Automotive CyberSecurity (ACS) reicht es nicht, nur die Prozesse eingeführt zu haben, sondern auch die Inhalte der Prozesse müssen stimmen, so dass Sicherheit gefördert wird. Daher ist es wichtig, dass die Audits von Experten mit fachlichen Kompetenzen hinsichtlich Cybersecurity und Entwicklungsprozessen in der Automobilindustrie begleitet werden. Ihr Urteil spielt dabei eine gewichtige Rolle für das Audit-Resultat.

Das VDA QMC bietet hierzu das Training „ACS-Experten für Automotive Cybersecurity-Managementsystem-Audits – Qualifizierung“ an. Entlang des VDA Bandes „ACSMS“ und der ISO 21434 werden die verschiedenen Fachthemen vermittelt und in umfangreichen Übungen vertieft. In Kleingruppen werden dabei unter anderem verschiedene Themen der Risikoanalyse und Bewertung von Prozessumsetzungen praktisch anhand von Beispielen geübt.





Ausblick

Die Veröffentlichung der ISO 21434 und die Umsetzung der UNECE 155 steigern nicht nur das Bewusstsein für Sicherheit im Auto (Automotive CyberSecurity), sondern fordern auch konkretes Handeln, um Typenzulassungen zu erreichen. Hiermit wird ein wesentlicher Grundstein für die verbesserte Sicherheit gelegt. Die Umsetzung bei allen beteiligten Firmen und das Zusammenspiel entlang der Lieferkette wird dazu eine besondere Relevanz bekommen.

Zum Nachweis der Einhaltung von Vorgaben werden dazu interne und externe Audits wachsende Bedeutung bekommen, erlauben sie doch den Nachweis der Einhaltung der einschlägigen Standards. Für die Durchführung wird der VDA-Band „ACSMS“ und die Ausbildung der ACS-Experten ein entscheidendes Fundament bilden.

Bei der Umsetzung der Standards werden Erfahrungen gesammelt werden, die gepaart mit dem Wissen, dass sich Cybersecurity permanent entwickelt, sicher dazu führen, dass es auch in Zukunft Weiterentwicklungen geben wird. Anpassungen und Updates sind daher zu erwarten und werden entsprechend auch beim VDA reflektiert werden.

Kontakte

Offene Schulungen
Telefon: +49 30 897842-252 und -253
E-Mail: seminare@vda-qmc.de

Inhouse Schulungen
Telefon: +49 30 897842-255
E-Mail: inhouse@vda-qmc.de

Live-Online-Schulungen
Telefon: +49 30 897842-257
E-Mail: seminare@vda-qmc.de

Schulungs-Lizenzpartner
Telefon: +49 30 897842-254 und -256
E-Mail: licence@vda-qmc.de



VDA QMC

Verband der Automobilindustrie
Qualitäts-Management-Center