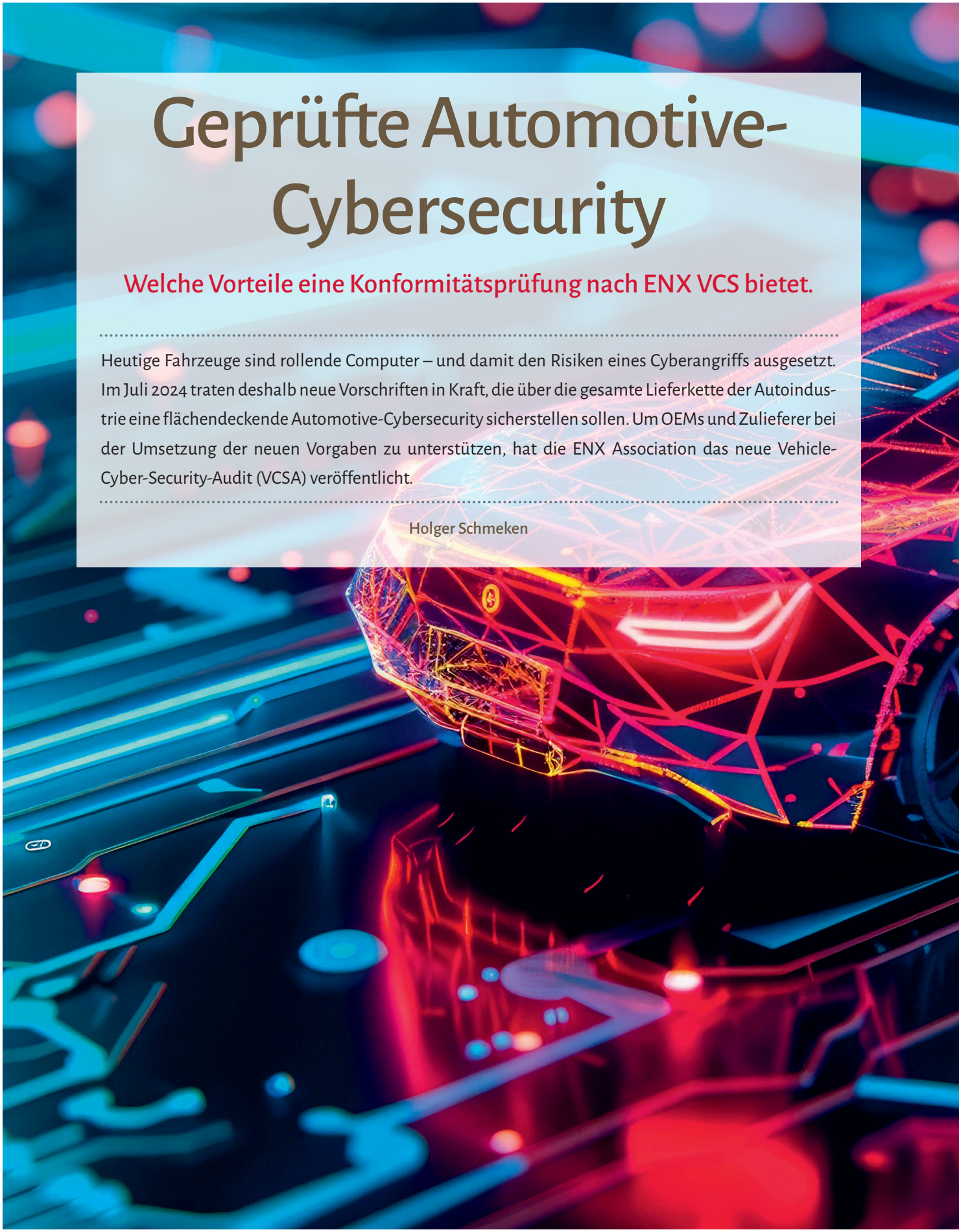


Geprüfte Automotive-Cybersecurity

Welche Vorteile eine Konformitätsprüfung nach ENX VCS bietet.

Heutige Fahrzeuge sind rollende Computer – und damit den Risiken eines Cyberangriffs ausgesetzt. Im Juli 2024 traten deshalb neue Vorschriften in Kraft, die über die gesamte Lieferkette der Autoindustrie eine flächendeckende Automotive-Cybersecurity sicherstellen sollen. Um OEMs und Zulieferer bei der Umsetzung der neuen Vorgaben zu unterstützen, hat die ENX Association das neue Vehicle-Cyber-Security-Audit (VCSA) veröffentlicht.

Holger Schmeken

Die digitale Transformation hat Fahrzeuge leistungsfähiger und sicherer gemacht. Durch elektronische Steuerungssysteme und ständige Vernetzung sind sie jedoch auch Zielscheiben für Cyberkriminelle geworden. Kritische Systeme könnten attackiert werden, was potenziell fatale Folgen haben kann. Trotz strengster Softwareentwicklungsstandards selbst in der Luftfahrt gibt es keine Garantie für fehlerfreie Software. Allerdings erlaubt die softwareseitige Steuerung eine schnelle Reaktion auf Qualitätsprobleme – Updates können heute Over-the-air (OTA) quasi über Nacht erfolgen.

Verbindliche Cybersecurity-Regularien

Um den zunehmenden Cyberbedrohungen zu begegnen, verabschiedeten die Vereinten Nationen die UNECE R 155 und 156, die die Implementierung eines Cyber Security Management Systems (CSMS) beziehungsweise eines Software Updates Management Systems (SUMS) beinhalten. Die Regelungen sollen die Cybersicherheit über den gesamten Lebenszyklus eines Modells und entlang der ganzen Lieferkette sicherstellen. In der EU sind die Vorschriften seit Juli 2024 für alle neu hergestellten Fahrzeuge verbindlich.

ENX VCS – weltweites Auditprogramm für ISO/SAE 21434

Mit der ISO/SAE 21434 (Road Vehicles – Cyber Security Engineering) wurde im Zuge der UN-Regularien versucht, einen Leitfaden und Konformitätsnachweis für die Erfüllung der Vorschriften zu schaffen. In der Praxis erwiesen sich die jeweiligen Auditprogramme der Prüfdienstleister jedoch als zu unterschiedlich – trotz der Spezifizierung durch die ISO/PAS 5112. Den Herstellern fehlte also nach wie vor die Möglichkeit, dem Gesetzgeber verlässliche und vergleichbare Belege über die Compliance-Konformität ihrer Supplier zu liefern – die ihrerseits wiederum Probleme hatten, die Einhaltung ihrer vertraglichen Bestimmungen auf Basis einer vergleichbaren Prüfgrundlage nachzuweisen.

Daher hat die ENX Association (ein Zusammenschluss europäischer Automobilhersteller, -Zulieferer und Verbände) das Auditprogramm ENX VCS konzipiert. ENX VCS prüft die Umsetzung eines Vehicle ›››

Cybersecurity im Automobilbau

Verschiedene Verordnungen, Normen und Regelwerke wurden in den letzten Jahren entwickelt, um Fahrzeuge bestmöglich vor Cyber-Bedrohungen zu schützen.

UN-Regulation Nr. 155 (UNECE WP.29)

Diese Verordnung fordert von Automobilherstellern die Implementierung eines Cyber-Security-Management-Systems (CSMS). Sie ist ein rechtlicher Rahmen, der garantieren soll, dass Fahrzeuge strengen Cybersicherheitsanforderungen entsprechen.

UN-Regulation Nr. 156 (UNECE WP.29)

Diese Verordnung ergänzt UN-Regulation Nr. 155 und bezieht sich auf sichere Software-Updates und das Software-Update-Management-System (SUMS). Fahrzeuge müssen in der Lage sein, sicherheitsrelevante Software Updates zu empfangen und zu installieren.

ISO/SAE 21434:2021 „Road vehicles – Cybersecurity engineering"

Diese Norm gilt für Komponenten (elektronische Bauteile und Software) von Fahrzeugen, die in Serie gefertigt werden, sowie Ersatz- und Zubehörteile. Sie definiert Anforderungen für die Cybersicherheit im gesamten Lebenszyklus eines Fahrzeugs, von der Entwicklung über die Produktion bis hin zu Wartung und Betrieb. Sie bietet einen Rahmen, der Herstellern hilft, Bedrohungen zu identifizieren, Risiken zu bewerten und Sicherheitsmaßnahmen zu implementieren.

ISO 26262:2018 „Road vehicles – Functional safety"

Diese Norm bezieht sich auf die funktionale Sicherheit von Straßenfahrzeugen und beinhaltet die Berücksichtigung von Cybersicherheitsaspekten als Teil der Risikobewertung. Sie soll dafür sorgen, dass sicherheitskritische Systeme im Fahrzeug zuverlässig funktionieren und Ausfälle minimiert werden.

IEC 62443 „IT-Sicherheit für Netze und Systeme"

Diese Normenreihe befasst sich mit der Cybersicherheit von industriellen Automatisierungs- und Steuerungssystemen.

Tisax (Trusted Information Security Assessment Exchange)

Tisax ist ein Standard für Informationssicherheit, der speziell für die Automobilindustrie entwickelt wurde.

Automotive Spice

Automotive Spice (Software Process Improvement and Capability dEtermination) ist ein Prozessbewertungsmodell, das speziell für die Automobilindustrie entwickelt wurde, um die Reife von Softwareentwicklungsprozessen zu bewerten.

Cyber Security Management Systems (V-CSMS) nach ISO 21434 und ISO 5112. Der entscheidende Vorteil: Das VCS-Audit ist weltweit standardisiert und lässt sich schneller an neue Herausforderungen anpassen als eine ISO-Norm. Eine Gruppe internationaler Experten überprüft das Auditprogramm regelmäßig, um es auf dem neuesten Stand zu halten.

Einheitliche Audits – vergleichbare Ergebnisse

Mit dem standardisierten ENX-VCS-Audit vermeiden Unternehmen unnötigen, nicht zuletzt finanziellen Aufwand, der bei multiplen Auditprozessen und divergierenden Prüfungen entstehen kann. Um global über alle Auditanbieter hinweg vergleichbare Abläufe zu gewährleisten, hat die ENX zum Launch des Programms auch konkrete Audit Provider Criteria & Assessment Requirements (ACAR VCS) sowie einen verbindlichen Prüfkatalog für Vehicle Cyber Security Audits (VCSA) veröffentlicht.

Dieser definiert für VCS-Auditoren eine Reihe obligatorischer Kompetenzen und ein verbindliches Vorgehensmodell – neben der organisatorischen Prüfung der V-CSMS-Regelungen etwa auch eine verpflichtende Dokumenten- und Prozessprüfung sowie die Bildung einer risikoorientierten Stichprobe aller Cyber Security-relevanten Projekte. Die Engineering-Teams, die für die Projekte der Stichprobe verantwortlich sind, werden anschließend von den Auditoren und Experten interviewt.

Arbeitsergebnisse des Teams werden gesichtet, um sicherzustellen, dass das V-CSMS auch tatsächlich in der Praxis Anwendung findet. Nach Abschluss der erfolgreichen Prüfung können die Unternehmen bei der ENX ein entsprechendes VCS-Label beantragen und über den Austauschmechanismus der ENX für interessierte Parteien zugänglich machen.

Tisax und VCS wirken im Tandem

Strukturell sind die VCS-Audits mit dem ACAR VCS an den etablierten Automobilstandard Tisax angelehnt. Beide Prüfmechanismen ergänzen sich: Während Tisax die Informationssicherheit in einem Unternehmen bewertet, bestätigt das VCS-Label die Cybersicherheit bei den Fahrzeugkomponenten.

INFORMATION & SERVICE

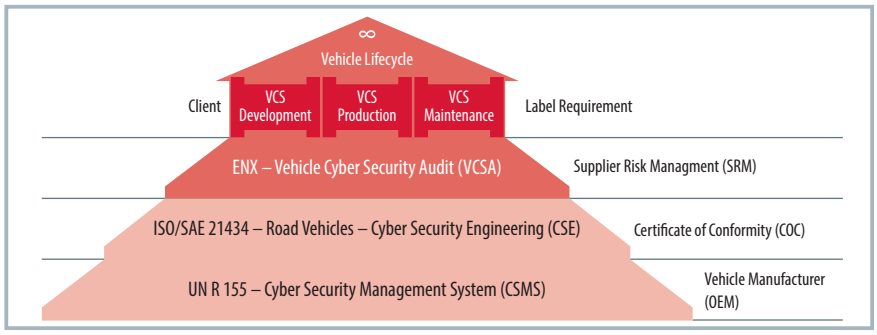
QUELLEN

ENX Association:
www.portal.enx.com/de-de/news/Introducing-Vehicle-Cybersecurity-VCS-Audit-scheme

AUTOR

Holger Schmeken ist Produktmanager der DQS GmbH für Tisax und VCS, Auditor für ISO/IEC 27001, Experte für Software Engineering mit mehr als 30 Jahren Erfahrung und stellvertretender Informationssicherheitsbeauftragter. Der Diplom-Wirtschaftsinformatiker verfügt ebenfalls über die erweiterte Auditkompetenz für kritische Infrastrukturen in Deutschland (Kritis).

KONTAKT



Das ENX-VCS-Label für Automotive-Cybersecurity deckt alle Ebenen von der regulatorischen Basis über die normativen Levels bis hin zur operativen Durchführung des VCS Audits ab. © DQS / Hanser

Ähnlich wie Tisax berücksichtigt das VCS-Audit die verschiedenen Rollen der Lieferanten bei der Bereitstellung von cyberrelevanten Komponenten. Jeder Lieferant muss daher nur die Anforderungen des VCSA-Prüfkatalogs erfüllen, die seiner tatsächlichen, spezifischen Rolle entsprechen. Dabei wird zwischen verschiedenen Labels unterschieden:

- **VCS Development:** Das Unternehmen führt die sichere Entwicklung von VCS Komponenten durch - von der Integration in die allgemeine Sicherheitsarchitektur, bis zur sicheren Implementierung und dem sicheren Übergang in die Produktion.
- **VCS Production:** Das Unternehmen produziert VCS-Komponenten und sorgt für deren sichere Konfiguration und Softwareausstattung.
- **VCS Operations & Maintenance:** Das Unternehmen ist mit Protokolldaten der Fahrzeugflotte betraut, die es erlauben problematische Betriebszustände oder konkrete Sicherheitsvorfälle zu identifizieren. Dieses Label eignet sich auch für Unternehmen, die ihre VCS Komponenten mittels Updates fortwährend aktuell halten müssen.

Konformitätsnachweis nach ENX VCS

Im Rahmen des VCS-Audits können OEMs und Zulieferer ihr V-CSMS bei zugelassenen Audit-Anbietern prüfen lassen und von der ENX ein drei Jahre gültiges VCS-Label erhalten. Die erhöhte globale Vergleichbarkeit der neuen Labels stärkt das Vertrauen in die Konformität des V-CSMS mit den Cyber-Sicherheitsvorgaben der UNECE R 155. So können Unternehmen ihre Compliance gegenüber Behörden und Geschäftspartnern eindeutig belegen und zur flächendeckenden Automotive Cybersecurity beitragen. Schnelles Handeln zahlt sich hier aus: Während der Einführungsphase ist die Registrierung für das ENX-VCS-Audit kostenfrei. ■