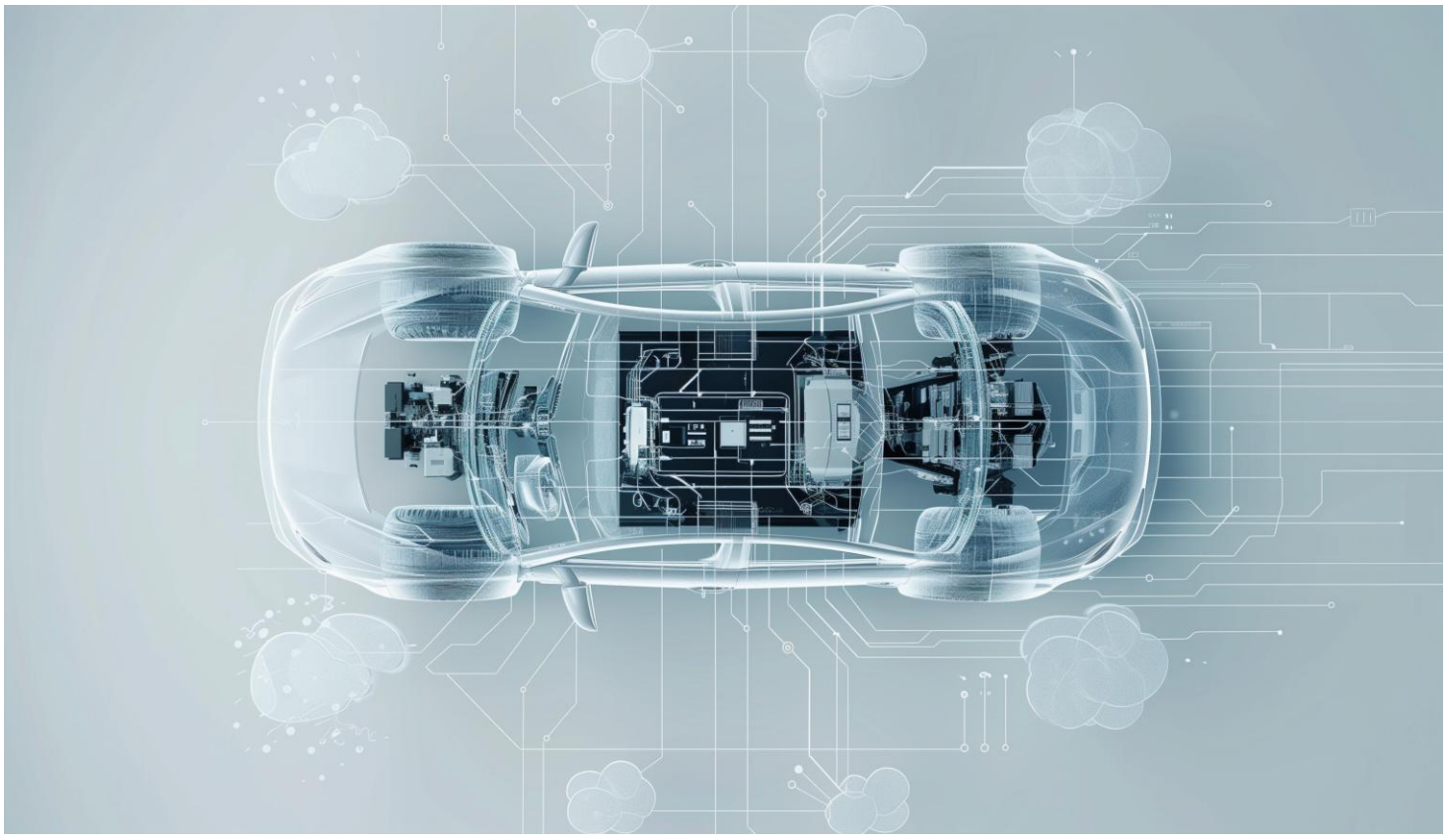
VDA Verband der Automobilindustrie

Position

End of Cybersecurity-Support (EoCSS)

Cybersicherheit für den Lebenszyklus



1. Einführung

Fahrzeuge verfügen zunehmend über vernetzte digitale Systeme und Komponenten, über die Fahrzeugfunktionen ausgeführt oder Systeme konfiguriert und aktualisiert werden können. Mit dem Grad der Vernetzung steigen auch die Wahrscheinlichkeit von Cyber-Angriffen sowie die daraus resultierenden Risiken. Als Voraussetzung für die Fahrzeug-Typzulassung schreibt die UNECE-Regelung155 (UN R155) Herstellern den Betrieb eines Cybersecurity-Managementsystems (CSMS) vor. Dieses umfasst organisatorische und prozessuale Vorgaben sowie technische Maßnahmen über den gesamten Produktlebenszyklus hinweg und reduziert dadurch die Auswirkungen von Cyber-Angriffen auf das Fahrzeug. Grundlagen einer langfristigen Cybersecurity von Fahrzeugen sind zum einen das Prinzip der „Security by Design“ in der Fahrzeugentwicklung sowie zum anderen risikobasierte Maßnahmen, die über die gesamte Lebensdauer des Fahrzeugs die Auswirkungen von Cyber-Angriffen reduzieren sollen. Die zentrale Herausforderung besteht darin, die Cybersecurity auch auf älteren Fahrzeugen aktuell zu halten, obwohl deren Komponenten und Systeme nicht mehr weiterentwickelt werden und ggfs. nicht mehr erweiterbar sind. Deshalb ist eine zeitlich klar definierte Cybersecurity-Supportphase erforderlich, die sich in der UN R155 finden sollte.

2. Abgleich der UN R155 mit relevanten Standards

Die in den nachfolgenden Kapiteln beschriebenen Vorgehensweisen und Konzepte basieren auf der UN R155 §7.2.2.1:

“The vehicle manufacturer shall demonstrate to an Approval Authority or Technical Service that their Cybersecurity Management System applies to the following phases: […] (c) Post-production phase“.

Eine Definition der im Kontext dieses Positionspapiers relevanten Post-production Phase ergibt sich aus UN R155 §2.7:

"Post-production phase" refers to the period in which a vehicle type is no longer produced until the end-of-life of all vehicles under the vehicle type. Vehicles incorporating a specific vehicle type will be operational during this phase but will no longer be produced. The phase ends when there are no longer any operational vehicles of a specific vehicle type.”

Ergänzt werden diese Klauseln durch das „Interpretation Document“ der UN R155, Absatz M, Erklärung der Anforderungen zu § 7.2.2 und § 7.2.2.1:

§ 7.2.2: *“The intention of this requirement is that the cybersecurity management system should be able to demonstrate how a manufacturer will handle cybersecurity during the operational life of vehicles produced under a vehicle type. This includes evidencing that there are procedures and processes implemented to cover the three phases. The different phases of the lifecycle may have specific activities to be performed in each of them.”*

§ 7.2.2.1: *“[...] The CSMS may include active and/or reactive processes or procedures covering the end of support for a vehicle type and how this is implemented or triggered. It may include the possibility to disconnect non-mandatory functions/systems and under what conditions this might happen. [...]”*

Somit müssen die Hersteller das CSMS in Zusammenarbeit mit ihren Zulieferern für eine zeitlich unbestimmte Periode betreiben, da die Post-production Phase erst endet, wenn das letzte Fahrzeug eines Fahrzeugtyps nicht mehr in Betrieb ist und damit sein „End-of-Life“ (EoL) erreicht ist.

Anders als in der UN R155 wird in der ISO/SAE 21434 nicht von „End-of-Life“ (EoL), sondern von

einer „End of Cybersecurity-Support“ (EoCSS) Phase gesprochen.

“Clause 8 (Continual cybersecurity activities) includes activities that provide information for ongoing risk assessments and defines vulnerability management of E/E systems until end of Cybersecurity-Support”.

“Clause 14 (End of Cybersecurity-Support and decommissioning) includes cybersecurity considerations for end of support and decommissioning of an item or component.”

Ein Vergleich mit verwandten Branchen ist hilfreich: Die ISO/WD 24882 “Agricultural machinery, tractors, and earth-moving machinery – Cybersecurity Engineering” vom 12.12.2024 sieht ein EoCSS und zwei „Operation Phases“ vor:

- “Operation Phase 1 – Manufacturing delivery to end of Cybersecurity-Support period […] The manufacturer shall monitor for events and handle the vulnerabilities”
- “Operation Phase 2 – end of Cybersecurity-Support to product decommissioning (end of life) […] The manufacturer may monitor for events and handle the vulnerabilities”

Diese Phase von „End-of-Production“ (EoP) bis EoCSS deckt nicht vollständig die von der UN R155 definierte Post-production Phase bis zum EoL ab. Demnach können sich die Prozesse und Aktivitäten bzw. Inhalte und Anforderungen für die Zeiträume von EoP bis EoCSS und von EoCSS bis EoL unterscheiden.

In diesem Kontext sind die Prozesse und Aktivitäten zwischen dem Fahrzeughersteller und seinen Lieferanten zu vereinbaren. Mindestanforderungen diesbezüglich sind weder in der UN R155 noch in der ISO/SAE 21434 beschrieben. Als Grundlage für diese Vereinbarungen sollten sich herausgebildete branchenübliche Vorgehensweisen genutzt werden.

3. Herausforderungen der Industrie durch diese Regelungen

Die Verpflichtung zum Erhalt der Cybersecurity im Fahrzeug bis zum EoL gemäß UN R155 stellt die Automobilindustrie vor erhebliche Herausforderungen. Der regulatorischen Anforderung, Fahrzeuge über deren gesamten Lebenszyklus hinweg gegen sich verändernde Cyberbedrohungen abzusichern, stehen technische Machbarkeit, organisatorische Umsetzbarkeit, rechtliche Klarheit und wirtschaftliche Tragfähigkeit gegenüber. Technische Herausforderungen ergeben sich insbesondere aus der zunehmenden Systemkomplexität und der sich stetig verändernden Bedrohungslage. Systeme, die heute entwickelt werden, müssen über möglichst lange Zeiträume hinweg gegenüber Angriffsszenarien geschützt werden, die zum Zeitpunkt der Entwicklung noch nicht erkennbar sind. Hersteller müssten den Umfang der Hardware, die zur Erfüllung der Anforderungen aus der UN R155 erforderlich ist, zu einem Zeitpunkt festlegen, zu dem die späteren Rahmenbedingungen noch gar nicht bekannt sein können. Daraus ergeben sich beispielhaft die folgenden Herausforderungen:

- Die Verfügbarkeit leistungsfähiger Rechenressourcen und neuer Technologien (wie Quantencomputing oder KI) ermöglicht künftig deutlich anspruchsvollere Angriffe. Dies erfordert wiederum neue Sicherheitslösungen, die insbesondere nach dem EoP technisch nicht mehr nachgerüstet werden können.
- Toolhersteller und Zulieferer von Standardsoftware bieten in der Regel nur einen zeitlich befristeten Cybersecurity Support. Gleiches gilt für Open Source Software. Dadurch ist eine quasi unbefristete Supportleistung für Cybersecurity durch

Hersteller für die Fahrzeuge technisch nicht realisierbar.

- Die Pflicht zur langfristigen Absicherung zwingt die Unternehmen zur Beibehaltung der zum Entwicklungszeitpunkt genutzten Technologien, z.B. der Toolchain. Dadurch werden rare hochqualifizierte Fachkräfte an veraltete Systeme gebunden und somit die volkswirtschaftliche Innovationskraft geschwächt.

Aufgrund der hier genannten Herausforderungen lässt sich der geforderte Cybersecurity-Support bis EoL faktisch nicht realisieren, auch nicht durch vertragliche Regelungen innerhalb der Lieferkette.

4. Forderungen hinsichtlich des Cybersecurity-Support-Zeitraums innerhalb des Fahrzeug-Lifecycles

Insbesondere im Hinblick auf technische Realisierbarkeit und wirtschaftliche Nachhaltigkeit zur Sicherstellung des Cybersecurity-Supports über den gesamten Produktlebenszyklus sind unterschiedliche Prozesse und Aktivitäten und eine differenzierte Behandlung der Elemente einer E/E Architektur für die Zeiträume bis EoCSS und danach bis EoL notwendig. Folgende Rahmenbedingungen sind notwendig:

- Ein EoCSS muss in die UN R155 aufgenommen werden. In der Phase nach EoP bis zum EoCSS umfasst der Cybersecurity-Support Prozesse und Aktivitäten, die jeweils zwischen den einzelnen Fahrzeugherstellern und den jeweiligen Zulieferern vereinbart werden.

- Der EoCSS soll sowohl für Elemente eines Fahrzeugs als auch für einen Fahrzeugtyp durch den jeweiligen Hersteller definiert werden können.

- Für eine aus Cybersecurity-Sicht differenzierte Behandlung der Elemente einer E/E Architektur sind diese in unterschiedliche Kategorien (s. Abbildung) einzuteilen, in denen aktive und/oder reaktive Aktivitäten unterschiedlich lange durchgeführt werden.

- Nach EoCSS bis EoL soll aus Cybersecurity-Sicht nur eine passive Produktbeobachtung im Rahmen der allgemeinen Produktbeobachtungspflicht des Herstellers durchgeführt werden müssen.

Im Detail bedeutet dies: Im Rahmen des Cybersecurity-Supports werden sowohl präventive/aktive als auch reaktive Maßnahmen, abhängig von einer Produktrisikobewertung, unterschiedlich lange durchgeführt.

Der aktive Cybersecurity-Support kann beispielsweise umfassen:

- Beobachtung von Security-bezogene Informationen („Threat Intelligence“), z.B. scannen von relevanten Verwundbarkeitsdatenbanken,

- Identifikation, Analyse und Klassifizierung von Verwundbarkeiten,

- Bewertung des Security-Risikos.

Dabei gilt vorsorgliches Handeln, d.h. angemessene Maßnahmen werden bei Kenntnis von einer (noch) nicht ausgenutzten Sicherheitslücke vorsorglich definiert.

Der reaktive Cybersecurity-Support kann beispielsweise das Bearbeiten von

- sicherheitsrelevanten Einzelfallmeldungen,
- Meldungen von Importeuren und Händlern an den Autohersteller,
- Kundenreklamationen und Beanstandungen oder
- Behördenbeanstandungen

umfassen. Dabei wird gezielt reagiert und es sollten angemessene Maßnahmen definiert werden, um auf ausgenutzte oder ausnutzbare Sicherheitslücken zu reagieren.

Die Elemente einer E/E Architektur sind in EoCSS Kategorien aufzuteilen, um eine differenzierte Behandlung zu ermöglichen. Diese Kategorien, sowie der Mindestzeitraum für den Cybersecurity-Support pro Kategorie, sollen in Abhängigkeit von Funktionen und Fahrzeugarchitektur durch den Hersteller des Gesamtfahrzeugs und/oder durch den Hersteller der Elemente festgelegt werden.

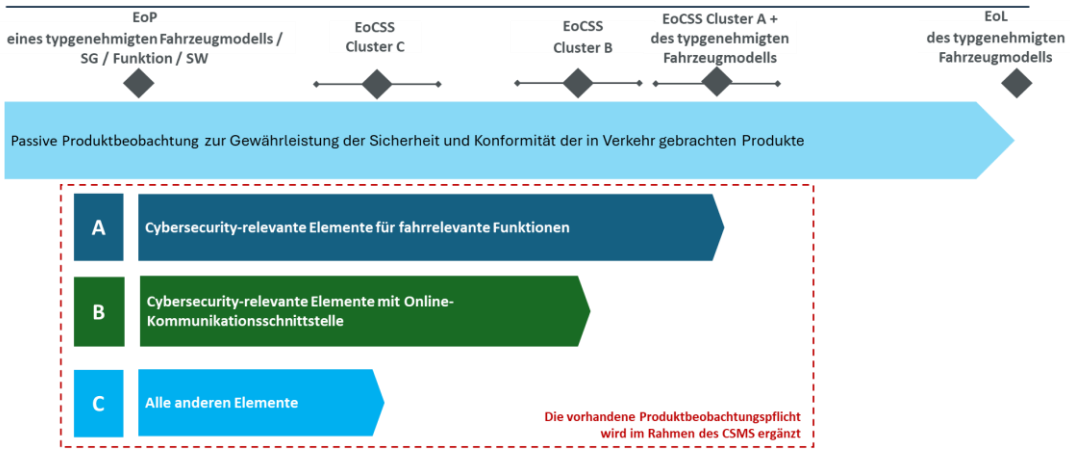


Abbildung: EoCSS Cluster/Kategorien (SG = Steuergerät, SW = Software)

Eine beispielhafte Kategorisierung könnte sein:

Kategorie A: Cybersecurity-relevante Elemente für fahrrelevante Funktionen, wie z.B. Elemente, die direkten Einfluss auf die zentralen Schutzziele des UN 1958er Abkommens (Safety, Environment, Theft Protection) und daher besonderen Schutzbedarf haben.

Kategorie B: Cybersecurity-relevante Elemente mit Online-Kommunikations-schnittstellen, wie z.B. Elemente mit WLAN, BT, 5G, …

Kategorie C: Cybersecurity-relevante Elemente deren Online-Komponente nicht zwingend ist und mobile Online-Dienste/Apps.

Nach Beendigung des Zeitraums in dem Cybersecurity-Support geleistet wird, beginnt die Phase zwischen dem EoCSS und EoL. Aus Cybersecurity-Sicht erfolgt in dieser Phase eine passive Produktbeobachtung im Rahmen der allgemeinen Produktbeobachtungspflicht des Unternehmens.

Nach EoCSS ist nicht mehr unbedingt sichergestellt, dass in den Unternehmen entlang der Lieferkette erforderliche Expertise und dazugehörige Werkzeuge bereitgestellt werden können.

5. Fazit

Die Anforderungen der UN R155 zur Absicherung der Cybersecurity über den gesamten Fahrzeuglebenszyklus stellen die Automobilindustrie vor faktisch nicht lösbare technische, organisatorische und wirtschaftliche Herausforderungen. Um einen praktikablen Ausgleich zwischen regulatorischen Vorgaben und industrieller Umsetzbarkeit zu schaffen, fordern wir eine Differenzierung zwischen einem aktiven Cybersecurity-Support bis zum End of Cybersecurity-Support (EoCSS) und einer passiven Beobachtungspflicht bis zum End-of-Life“ (EoL):

- Aufnahme eines EoCSS in die UN R155
- Definition EoCSS der Elemente durch den jeweiligen Hersteller
- Einteilung der Elemente einer E/E Architektur in unterschiedliche EoCSS Kategorien
- Nach EoCSS bis EoL nur noch passive Produktbeobachtung.

Nur durch eine definierte und gesetzlich abgestimmte Vorgehensweise kann der geforderte Schutz von Fahrzeugen über ihren Lebenszyklus hinweg sichergestellt und der Schutz des Kunden gewährleistet werden, ohne die Innovationsfähigkeit und Wirtschaftlichkeit der Industrie zu gefährden.

Ansprechpartner

Dr. Marcus Bollig
Geschäftsführer
marcus.bollig@vda.de

Martin Lorenz
Abteilungsleiter
Security, Daten &Digitalisierung
martin.lorenz@vda.de

Dr. Kirsten Matheus
Referentin
kirsten.matheus@vda.de

Der Verband der Automobilindustrie (VDA) vereint mehr als 620 Hersteller und Zulieferer unter einem Dach. Die Mitglieder entwickeln und produzieren Pkw und Lkw, Software, Anhänger, Aufbauten, Busse, Teile und Zubehör sowie immer neue Mobilitätsangebote.

Wir sind die Interessenvertretung der Automobilindustrie und stehen für eine moderne, zukunftsorientierte multimodale Mobilität auf dem Weg zur Klimaneutralität. Der VDA vertritt die Interessen seiner Mitglieder gegenüber Politik, Medien und gesellschaftlichen Gruppen.

Wir arbeiten für Elektromobilität, klimaneutrale Antriebe, die Umsetzung der Klimaziele, Rohstoffsicherung, Digitalisierung und Vernetzung sowie German Engineering. Wir setzen uns dabei für einen wettbewerbsfähigen Wirtschafts- und Innovationsstandort ein. Unsere Industrie sichert Wohlstand in Deutschland: Mehr als 740.000 Menschen sind, direkt in der deutschen Automobilindustrie beschäftigt.

Der VDA ist Veranstalter der größten internationalen Mobilitätsplattform IAA MOBILITY und der IAA TRANSPORTATION, der weltweit wichtigsten Plattform für die Zukunft der Nutzfahrzeugindustrie.

Herausgeber	Verband der Automobilindustrie e. V. (VDA) Behrenstraße 35, 10117 Berlin www.vda.de Deutscher Bundestag Lobbyregister-Nr.: R001243 EU-Transparenz-Register-Nr.: 9557 4664 768-90
Copyright	Verband der Automobilindustrie e. V. (VDA) Nachdruck und jede sonstige Form der Vervielfältigung ist nur mit Angabe der Quelle gestattet
Version	November 2025