Amtsblatt
der Europäischen Union

DE
Reihe L

2025/5

10.1.2025

Nur die von der UN/ECE verabschiedeten Originalfassungen sind international rechtsverbindlich. Der Status dieser Regelung und das Datum ihres Inkrafttretens sind der neuesten Fassung des UN/ECE-Statusdokuments TRANS/WP.29/343 zu entnehmen, das von folgender Website abgerufen werden kann: https://unece.org/status-1958-agreement-and-annexed-regulations

UN-Regelung Nr. 155 — Einheitliche Bedingungen für die Genehmigung von Fahrzeugen hinsichtlich der Cybersicherheit und des Cybersicherheitsmanagementsystems [2025/5]

Einschließlich des gesamten gültigen Textes bis:

Ergänzung 3 zur Regelung in der ursprünglichen Fassung — Tag des Inkrafttretens: 10. Januar 2025

Dieses Dokument ist lediglich eine Dokumentationsquelle. Die rechtsverbindlichen Originaltexte sind:

— ECE/TRANS/WP.29/2020/79 (geändert durch ECE/TRANS/WP.29/2020/94 und ECE/TRANS/WP.29/2020/97)

— ECE/TRANS/WP.29/2022/54

— ECE/TRANS/WP.29/2023/70 und

— ECE/TRANS/WP.29/2024/55

INHALT

Regelung

1. Anwendungsbereich
2. Begriffsbestimmungen
3. Antrag auf Genehmigung
4. Kennzeichnungen
5. Genehmigung
6. Konformitätsbescheinigung für das Cybersicherheitsmanagementsystem
7. Vorschriften
8. Änderung des Fahrzeugtyps und Erweiterung der Typgenehmigung
9. Übereinstimmung der Produktion
10. Maßnahmen bei Abweichungen der Produktion
11. Endgültige Einstellung der Produktion
12. Namen und Anschriften der technischen Dienste, die die Prüfungen für die Genehmigung durchführen, und der Typgenehmigungsbehörden

Anlagen

1 Beschreibungsbogen

2 Mitteilung

3 Anordnung des Genehmigungszeichens

4 Muster einer Konformitätsbescheinigung für ein CSMS

5 Liste der Bedrohungen und der entsprechenden Minderungsmaßnahmen

1. Anwendungsbereich

1.1. Diese Regelung gilt hinsichtlich der Cybersicherheit für Fahrzeuge der Klassen L, M, N und O, wenn diese mit mindestens einem elektronischen Steuergerät ausgestattet sind.

1.2. Diese Regelung gilt unbeschadet anderer UN-Regelungen sowie regionaler oder nationaler Rechtsvorschriften, die den Zugang befugter Parteien zu dem Fahrzeug, dessen Daten, Funktionen und Ressourcen sowie die Zugangsbedingungen regeln. Sie gilt auch unbeschadet der Anwendung nationaler und regionaler Rechtsvorschriften zum Schutz der Privatsphäre und zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten.

1.3. Diese Regelung gilt unbeschadet anderer UN-Regelungen sowie nationaler oder regionaler Rechtsvorschriften, die die Entwicklung und Installation/Systemintegration sowohl physischer als auch digitaler Ersatzteile und Bauteile im Hinblick auf die Cybersicherheit regeln.

2. Begriffsbestimmungen

Für die Zwecke dieser Regelung gelten folgende Begriffsbestimmungen:

2.1. „Fahrzeugtyp“ bezeichnet Fahrzeuge, die sich zumindest in folgenden wesentlichen Punkten nicht voneinander unterscheiden:

a) vom Hersteller angegebene Bezeichnung des Fahrzeugtyps,

b) wesentliche Aspekte der elektrischen/elektronischen Architektur und der externen Schnittstellen hinsichtlich der Cybersicherheit.

2.2. „Cybersicherheit“ bezeichnet den Zustand, in dem Straßenfahrzeuge und deren Funktionen vor Cyberbedrohungen für elektrische oder elektronische Bauteile geschützt sind.

2.3. „Cybersicherheitsmanagementsystem (CSMS)“ bezeichnet einen systematischen, risikobasierten Ansatz zur Festlegung von organisatorischen Abläufen, Zuständigkeiten und Governance beim Umgang mit Risiken im Zusammenhang mit Cyberbedrohungen für Fahrzeuge und beim Schutz von Fahrzeugen vor Cyberangriffen.

2.4. „System“ bezeichnet einen Satz von Bauteilen und/oder Subsystemen, mit dem eine oder mehrere Funktionen implementiert werden.

2.5. „Entwicklungsphase“ bezeichnet den Zeitraum vor der Typgenehmigung eines Fahrzeugtyps.

2.6. „Produktionsphase“ bezeichnet den Zeitraum, in dem ein Fahrzeugtyp hergestellt wird.

2.7. „Post-Produktionsphase“ bezeichnet den Zeitraum ab dem Zeitpunkt, zu dem ein Fahrzeugtyp nicht mehr hergestellt wird, bis zum Ende der Lebensdauer aller Fahrzeuge dieses Fahrzeugtyps. In dieser Phase sind Fahrzeuge eines bestimmten Fahrzeugtyps zwar betriebsfähig, werden aber nicht mehr hergestellt. Die Phase endet, wenn es keine betriebsfähigen Fahrzeuge des betreffenden Fahrzeugtyps mehr gibt.

2.8. „Minderungsmaßnahme“ bezeichnet eine Maßnahme, die ein Risiko verringert.

2.9. „Risiko“ bezeichnet die Möglichkeit, dass durch eine bestimmte Bedrohung Schwachstellen eines Fahrzeugs ausgenutzt werden und dadurch einer Organisation oder einer Person Schaden zugefügt wird.

2.10. „Risikobewertung“ bezeichnet den gesamten Prozess der Feststellung, Erkennung und Beschreibung von Risiken (Risikoermittlung), der Erfassung der Risikoart und der Bestimmung des Risikograds (Risikoanalyse) und des Vergleichs der Ergebnisse der Risikoanalyse mit bestimmten Risikokriterien, um festzustellen, ob das Risiko und/oder dessen Ausmaß akzeptabel bzw. tolerierbar ist (Risikoeinschätzung).

2.11. „Risikomanagement“ bezeichnet koordinierte Tätigkeiten zur Leitung und Kontrolle einer Organisation in Bezug auf ein Risiko.

2.12. „Bedrohung“ bezeichnet eine potenzielle Ursache eines unerwünschten Vorfalls, der zur Schädigung eines Systems, einer Organisation oder einer Person führen kann.

2.13. „Schwachstelle“ bezeichnet eine Schwäche eines Elements oder einer Minderungsmaßnahme, die durch eine oder mehrere Bedrohungen ausgenutzt werden kann.

3. Antrag auf Genehmigung

3.1. Der Antrag auf Erteilung einer Genehmigung für einen Fahrzeugtyp hinsichtlich der Cybersicherheit ist vom Fahrzeughersteller oder seinem ordentlich bevollmächtigten Vertreter einzureichen.

3.2. Diesem Antrag sind die nachstehend genannten Dokumente in dreifacher Ausfertigung und mit folgenden Angaben beizufügen:

3.2.1. Eine Beschreibung des Fahrzeugtyps unter Beachtung der in Anhang 1 dieser Regelung genannten Positionen.

3.2.2. Falls an den Beschreibungen nachweislich geistige Eigentumsrechte bestehen oder mit ihnen nachweislich spezifisches Know-how des Herstellers oder seiner Zulieferer preisgegeben wird, übermitteln der Hersteller oder seine Zulieferer Informationen, die für die in dieser Regelung genannten Überprüfungen ausreichend sind. Diese Informationen sind vertraulich zu behandeln.

3.2.3. Die Konformitätsbescheinigung für das CSMS gemäß Absatz 6 dieser Regelung.

3.3. Die Dokumentation muss zwei Teile umfassen:

a) Die förmliche Dokumentation für die Genehmigung, einschließlich der in Anhang 1 genannten Unterlagen, die der Genehmigungsbehörde oder dem technischen Dienst zum Zeitpunkt der Einreichung des Antrags auf Typgenehmigung vorzulegen ist. Diese Dokumentation dient der Genehmigungsbehörde oder ihrem technischen Dienst als Grundlage für das Genehmigungsverfahren. Die Genehmigungsbehörde oder ihr technischer Dienst stellt sicher, dass das Dokumentationspaket mindestens zehn Jahre ab dem Zeitpunkt, zu dem die Produktion des Fahrzeugtyps endgültig eingestellt wird, verfügbar bleibt.

b) Zusätzliches Material, das für die Vorschriften dieser Regelung von Bedeutung ist, kann vom Hersteller aufbewahrt werden, ist zum Zeitpunkt der Typgenehmigung jedoch zur Prüfung offenzulegen. Der Hersteller stellt sicher, dass das gesamte, zum Zeitpunkt der Typgenehmigung offengelegte Material für einen Zeitraum von mindestens zehn Jahren ab dem Zeitpunkt, zu dem die Produktion des Fahrzeugtyps endgültig eingestellt wird, verfügbar bleibt.

4. Kennzeichnung

4.1. An jedem Fahrzeug, das einem nach dieser Regelung genehmigten Fahrzeugtyp entspricht, ist sichtbar und an gut zugänglicher Stelle, die im Genehmigungsblatt anzugeben ist, ein internationales Genehmigungszeichen anzubringen, bestehend aus

4.1.1. einem Kreis, in dem sich der Buchstabe „E“ und die Kennzahl des Landes befinden, das die Genehmigung erteilt hat;

4.1.2. der Nummer dieser Regelung mit dem nachgestellten Buchstaben „R“, einem Bindestrich und der Genehmigungsnummer rechts neben dem Kreis nach Absatz 4.1.1.

4.2. Entspricht das Fahrzeug einem Fahrzeugtyp, der in dem Land, das die Typgenehmigung nach dieser Regelung erteilt hat, auch nach einer oder mehreren anderen Regelungen zum Übereinkommen genehmigt wurde, braucht das Zeichen nach Absatz 4.1.1 nicht wiederholt zu werden; in diesem Fall sind die Regelungs- und Genehmigungsnummern und die zusätzlichen Zeichen aller Regelungen, aufgrund deren die Genehmigung in dem Land erteilt wurde, das die Genehmigung nach dieser Regelung erteilt hat, untereinander rechts neben dem Zeichen nach Absatz 4.1.1 anzuordnen.

4.3. Das Genehmigungszeichen muss deutlich lesbar und dauerhaft sein.

4.4. Das Genehmigungszeichen ist auf dem vom Hersteller angebrachten Typenschild des Fahrzeugs oder in dessen Nähe anzugeben.

4.5. Anhang 3 dieser Regelung enthält Beispiele für die Anordnung des Genehmigungszeichens.

5. Genehmigung

5.1. Genehmigungsbehörden dürfen Typgenehmigungen hinsichtlich der Cybersicherheit nur für solche Fahrzeugtypen erteilen, die den Vorschriften dieser Regelung genügen.

5.1.1. Die Genehmigungsbehörde oder der technische Dienst überprüft mittels Dokumentenkontrollen, ob der Fahrzeughersteller die für den Fahrzeugtyp relevanten Maßnahmen ergriffen hat, die nötig sind, um Folgendes sicherzustellen:

a) Erfassung und Überprüfung der gemäß dieser Regelung erforderlichen Informationen über die gesamte Lieferkette hinweg, um nachzuweisen, dass lieferantenbezogene Risiken ermittelt und bewältigt werden;

b) Dokumentation der Risikobewertung (während der Entwicklungsphase oder nachträglich), der Testergebnisse und der Minderungsmaßnahmen bezogen auf den Fahrzeugtyp, einschließlich konstruktionsbezogener Informationen zur Untermauerung der Risikobewertung;

c) Implementierung geeigneter Cybersicherheitsmaßnahmen bei der Konzeption des Fahrzeugtyps;

d) Erkennung von und Reaktion auf mögliche Cyberangriffe;

e) Protokollierung von Daten zur Unterstützung der Erkennung von Cyberangriffen und Bereitstellung von Datenforensik, um eine Analyse versuchter oder erfolgreicher Cyberangriffe zu ermöglichen.

5.1.2. Die Genehmigungsbehörde oder der technische Dienst überprüft anhand von Tests an einem Fahrzeug des betreffenden Fahrzeugtyps, ob der Fahrzeughersteller die von ihm dokumentierten Cybersicherheitsmaßnahmen implementiert hat. Die entsprechenden Tests sind von der Genehmigungsbehörde oder dem technischen Dienst selbst oder in Zusammenarbeit mit dem Fahrzeughersteller mittels stichprobenartiger Überprüfungen durchzuführen. Die Stichproben sollen schwerpunktmäßig, aber nicht ausschließlich auf Risiken ausgerichtet sein, die zum Zeitpunkt der Risikobewertung als hoch eingeschätzt werden.

5.1.3. Die Genehmigungsbehörde oder der technische Dienst versagt die Erteilung der Typgenehmigung hinsichtlich der Cybersicherheit, wenn der Fahrzeughersteller eine oder mehrere der in Absatz 7.3 genannten Vorschriften nicht erfüllt hat, insbesondere folgende:

a) Der Fahrzeughersteller hat die laut Absatz 7.3.3 vorgesehene erschöpfende Risikobewertung nicht durchgeführt; dies ist auch dann der Fall, wenn der Hersteller nicht alle Risiken im Zusammenhang mit den in Anhang 5 Teil A genannten Bedrohungen berücksichtigt hat.

b) Der Fahrzeughersteller hat den Fahrzeugtyp nicht gegen die in der Risikobewertung des Fahrzeugherstellers ermittelten Risiken geschützt oder es wurden keine angemessenen Minderungsmaßnahmen gemäß Absatz 7 vorgesehen.

c) Der Fahrzeughersteller hat keine angemessenen und verhältnismäßigen Maßnahmen ergriffen, um bestimmte Umgebungen des Fahrzeugtyps (falls vorhanden) in Bezug auf die Speicherung und Ausführung von Software, Diensten, Anwendungen oder Daten des Anschlussmarktes zu sichern.

d) Der Fahrzeughersteller hat vor der Genehmigung keine angemessenen und ausreichenden Tests durchgeführt, um die Wirksamkeit der implementierten Sicherheitsmaßnahmen zu überprüfen.

5.1.4. Die bewertende Genehmigungsbehörde versagt die Typgenehmigung hinsichtlich der Cybersicherheit auch dann, wenn die Genehmigungsbehörde oder der technische Dienst vom Fahrzeughersteller keine ausreichenden Informationen zur Bewertung der Cybersicherheit des Fahrzeugtyps erhalten hat.

5.2. Über die Erteilung oder Erweiterung oder Versagung einer Genehmigung für einen Fahrzeugtyp nach dieser Regelung sind die Vertragsparteien des Übereinkommens von 1958, die diese Regelung anwenden, mit einem Mitteilungsblatt zu unterrichten, das dem Muster in Anhang 2 dieser Regelung entspricht.

5.3. Die Genehmigungsbehörden erteilen keine Typgenehmigung, ohne zuvor zu überprüfen, ob der Hersteller angemessene Vorkehrungen und Verfahren eingeführt hat, um den unter diese Regelung fallenden Aspekten der Cybersicherheit ordnungsgemäß Rechnung zu tragen.

5.3.1. Die Genehmigungsbehörde und ihre technischen Dienste stellen zusätzlich zu den in Verzeichnis 2 des Übereinkommens von 1958 festgelegten Kriterien sicher, dass die Hersteller über Folgendes verfügen:

a) Fachpersonal mit entsprechenden Kompetenzen im Bereich der Cybersicherheit und Fachkenntnissen bezüglich Risikobewertungen im Automobilbereich ([1]);

b) implementierte Verfahren für die einheitliche Bewertung gemäß dieser Regelung.

5.3.2. Jede Vertragspartei, die diese Regelung anwendet, unterrichtet über ihre Genehmigungsbehörde die Genehmigungsbehörden der anderen Vertragsparteien, die diese UN-Regelung anwenden, über das Verfahren und die Kriterien, die von der unterrichtenden Behörde zugrunde gelegt werden, um die Angemessenheit der Maßnahmen zu bewerten, die gemäß dieser Regelung, insbesondere gemäß den Absätzen 5.1, 7.2 und 7.3, getroffen werden.

Diese Informationen werden (a) nur vor der erstmaligen Erteilung einer Genehmigung nach dieser Regelung und (b) bei jeder Aktualisierung des Verfahrens oder der Kriterien für die Bewertung übermittelt.

Die Informationen sollen zwecks Erfassung und Analyse bewährter Verfahren und zur Sicherstellung einer konvergierenden Anwendung dieser Regelung durch alle Genehmigungsbehörden, die diese Regelung anwenden, gemeinsam genutzt werden.

5.3.3. Die Informationen gemäß Absatz 5.3.2 sind in englischer Sprache rechtzeitig und spätestens 14 Tage vor der erstmaligen Erteilung einer Genehmigung nach den betreffenden Bewertungsverfahren und -kriterien in die von der Wirtschaftskommission der Vereinten Nationen für Europa errichtete, sichere Internet-Datenbank DETA ([2]) hochzuladen. Die Informationen müssen hinreichend Aufschluss darüber geben, welche Mindestleistungsniveaus die Genehmigungsbehörde für die jeweiligen spezifischen Anforderungen gemäß Absatz 5.3.2 festgelegt hat und welche Verfahren und Maßnahmen sie anwendet, um zu überprüfen, ob diese Mindestleistungsniveaus erfüllt sind ([3]).

5.3.4. Genehmigungsbehörden, die die in Absatz 5.3.2 genannten Informationen erhalten, können der unterrichtenden Genehmigungsbehörde innerhalb von 14 Tagen nach dem Tag der Unterrichtung Bemerkungen übermitteln, die sie in DETA hochladen.

5.3.5. Kann die Genehmigungsbehörde, die die Genehmigung erteilt hat, die nach Absatz 5.3.4 eingegangenen Bemerkungen nicht berücksichtigen, so bemühen sich die Genehmigungsbehörden, die Bemerkungen übermittelt haben, und die Genehmigungsbehörde, die die Genehmigung erteilt hat, gemäß dem Verzeichnis 6 des Übereinkommens von 1958 um weitere Klärung. Die für diese Regelung zuständige nachgeordnete Arbeitsgruppe ([4]) des Weltforums für die Harmonisierung der Regelungen für Kraftfahrzeuge (WP.29) muss sich auf eine gemeinsame Auslegung der Bewertungsverfahren und -kriterien einigen ([5]). Diese gemeinsame Auslegung ist umzusetzen, und alle Genehmigungsbehörden müssen dementsprechend Typgenehmigungen im Rahmen dieser Regelung erteilen.

([1]) Z. B. ISO 26262-2018, ISO/PAS 21448, ISO/SAE 21434.
([2]) https://www.unece.org/trans/main/wp29/datasharing.html.
([3]) Anleitungen zu den im Einzelnen hochzuladenden Informationen (z. B. Verfahren, Kriterien, Leistungsniveau) und zum Format werden in dem Auslegungsdokument enthalten sein, das von der Taskforce für Cybersicherheit und Fragen der Drahtlosübertragung für die siebte Sitzung der Arbeitsgruppe „Automatisierte/autonome und vernetzte Fahrzeuge“ (GRVA) derzeit erstellt wird.
([4]) Die Arbeitsgruppe „Automatisierte/autonome und vernetzte Fahrzeuge“ (GRVA).
([5]) Diese Auslegung ist in dem in der Fußnote zu Absatz 5.3.3 angegebenen Auslegungsdokument wiederzugeben.

5.3.6. Jede Genehmigungsbehörde, die eine Typgenehmigung nach dieser Regelung erteilt, hat die anderen Genehmigungsbehörden darüber zu unterrichten. Die Genehmigungsbehörde lädt die Typgenehmigung zusammen mit der ergänzenden Dokumentation innerhalb von 14 Tagen nach dem Tag der Erteilung in englischer Sprache in DETA ([6]) hoch.

5.3.7. Die Vertragsparteien können die erteilten Genehmigungen anhand der gemäß Absatz 5.3.6 hochgeladenen Informationen untersuchen. Etwaige Meinungsverschiedenheiten zwischen den Vertragsparteien sind gemäß Artikel 10 und Verzeichnis 6 des Übereinkommens von 1958 beizulegen. Die Vertragsparteien unterrichten auch die zuständige nachgeordnete Arbeitsgruppe des Weltforums für die Harmonisierung der Regelungen für Kraftfahrzeuge (WP.29) über die abweichenden Auslegungen im Sinne von Verzeichnis 6 des Übereinkommens von 1958. Die zuständige Arbeitsgruppe unterstützt die Beilegung der Meinungsverschiedenheiten und kann sich hierzu erforderlichenfalls mit der WP.29 beraten.

5.4. Für die Zwecke des Absatzes 7.2 dieser Regelung stellt der Hersteller sicher, dass den unter diese Regelung fallenden Aspekten der Cybersicherheit Rechnung getragen wird.

6. Konformitätsbescheinigung für das Cybersicherheitsmanagementsystem

6.1. Die Vertragsparteien benennen eine Genehmigungsbehörde, die die Bewertung des Herstellers durchführen und eine Konformitätsbescheinigung für das CSMS ausstellen soll.

6.2. Ein Antrag auf Erteilung einer Konformitätsbescheinigung für das Cybersicherheitsmanagementsystem ist vom Fahrzeughersteller oder seinem ordentlich bevollmächtigten Vertreter einzureichen.

6.3. Dem Antrag sind die nachstehend genannten Dokumente in dreifacher Ausfertigung beizufügen, insbesondere:

6.3.1. Beschreibungen des Cybersicherheitsmanagementsystems;

6.3.2. Eine unterschriebene Erklärung nach dem Muster in Anlage 1 Anhang 1.

6.4. Im Rahmen der Bewertung muss der Hersteller unter Verwendung des in Anhang 1 Anlage 1 enthaltenen Musters erklären und der Genehmigungsbehörde oder deren technischem Dienst gegenüber in zufriedenstellender Weise nachweisen, dass er über die erforderlichen Verfahren verfügt, um alle Anforderungen an die Cybersicherheit im Sinne dieser Regelung zu erfüllen.

6.5. Wenn die Bewertung zufriedenstellend abgeschlossen wurde und eine unterzeichnete Erklärung des Herstellers gemäß dem Muster in Anhang 1 Anlage 1 eingegangen ist, wird dem Hersteller eine Bescheinigung mit der Bezeichnung „Konformitätsbescheinigung für ein CSMS“ gemäß dem Muster in Anhang 4 dieser Regelung erteilt.

6.6. Die Genehmigungsbehörde oder ihr technischer Dienst stellt die Konformitätsbescheinigung für das CSMS nach dem in Anhang 4 dieser Regelung enthaltenen Muster aus.

6.7. Die Konformitätsbescheinigung für das CSMS bleibt maximal drei Jahre ab Ausstellungsdatum gültig, sofern sie nicht zurückgenommen wird.

6.8. Die Genehmigungsbehörde, die die Konformitätsbescheinigung für das CSMS erteilt hat, kann jederzeit überprüfen, ob die diesbezüglichen Anforderungen weiterhin erfüllt sind. Die Genehmigungsbehörde muss die Konformitätsbescheinigung für das CSMS zurücknehmen, wenn die in dieser Regelung festgelegten Anforderungen nicht mehr erfüllt sind.

([6]) Weitere Informationen zu den Mindestanforderungen an das Dokumentationspaket werden von der GRVA auf ihrer siebten Sitzung erarbeitet.

6.9. Der Hersteller muss die Genehmigungsbehörde oder ihren technischen Dienst über jede Änderung informieren, die sich auf die Einschlägigkeit der Konformitätsbescheinigung für das CSMS auswirkt. Nach Rücksprache mit dem Hersteller entscheidet die Genehmigungsbehörde oder der technische Dienst, ob neue Prüfungen erforderlich sind.

6.10. Die Ausstellung einer neuen oder die Verlängerung der vorhandenen Konformitätsbescheinigung für das CSMS muss vom Hersteller rechtzeitig beantragt werden, d. h. die Genehmigungsbehörde muss Gelegenheit haben, noch vor Ablauf der Gültigkeitsdauer der vorhandenen Konformitätsbescheinigung für das CSMS ihre Bewertung abzuschließen. Vorbehaltlich einer positiven Bewertung stellt die Genehmigungsbehörde eine neue Konformitätsbescheinigung für das CSMS aus oder verlängert die Gültigkeit der vorhandenen Konformitätsbescheinigung um weitere drei Jahre. Die Genehmigungsbehörde überprüft, ob das CSMS weiterhin die Vorschriften dieser Regelung erfüllt. Die Genehmigungsbehörde stellt eine neue Bescheinigung aus, wenn der Genehmigungsbehörde oder dem technischen Dienst Änderungen mitgeteilt wurden und die Neubewertung positiv ausfällt.

6.11. Der Ablauf oder die Rücknahme der Konformitätsbescheinigung des Herstellers für das CSMS gilt in Bezug auf die Fahrzeugtypen, für die das betreffende CSMS maßgeblich war, als Änderung im Sinne von Absatz 8, was dazu führen kann, dass die Genehmigung zurückgenommen wird, wenn die Bedingungen für ihre Erteilung nicht mehr erfüllt sind.

7. Vorschriften

7.1. Allgemeine Vorschriften

7.1.1. Die Vorschriften dieser Regelung dürfen die Bestimmungen oder Vorschriften anderer UN-Regelungen nicht einschränken.

7.2. Anforderungen an das Cybersicherheitsmanagementsystem

7.2.1. Im Zuge der Bewertung muss die Genehmigungsbehörde oder ihr technischer Dienst überprüfen, ob der Fahrzeughersteller ein Cybersicherheitsmanagementsystem installiert hat und ob dieses System die Vorschriften der vorliegenden Regelung erfüllt.

7.2.2. Das Cybersicherheitsmanagementsystem soll folgenden Aspekten Rechnung tragen:

7.2.2.1. Der Fahrzeughersteller muss gegenüber einer Genehmigungsbehörde oder einem technischen Dienst darlegen, dass sein Cybersicherheitsmanagementsystem in folgenden Phasen anwendbar ist:

a) Entwicklungsphase

b) Produktionsphase

c) Post-Produktionsphase.

7.2.2.2. Der Fahrzeughersteller muss nachweisen, dass bei den Verfahren im Rahmen seines Cybersicherheitsmanagementsystems gewährleistet ist, dass dem Aspekt der Sicherheit angemessen Rechnung getragen wird; hier sind auch die in Anhang 5 aufgeführten Risiken und Minderungsmaßnahmen zu berücksichtigen. Dies umfasst:

a) die Verfahren, die innerhalb der Organisation des Herstellers für das Cybersicherheitsmanagement eingesetzt werden;

b) die Verfahren, die zur Ermittlung von Risiken für Fahrzeugtypen eingesetzt werden. Im Rahmen dieser Verfahren werden die in Anhang 5 Teil A aufgeführten Bedrohungen sowie weitere einschlägige Bedrohungen betrachtet;

c) die Verfahren zur Bewertung, Kategorisierung und Behandlung der ermittelten Risiken;

d) die Verfahren, mit denen überprüft wird, ob ein angemessenes Management der ermittelten Risiken erfolgt;

e) die Verfahren zum Testen der Cybersicherheit eines Fahrzeugtyps;

f) die Verfahren zur Sicherstellung einer kontinuierlich aktualisierten Risikobewertung;

g) die Verfahren zur Überwachung und Erkennung von Cyberangriffen, Cyberbedrohungen und Schwachstellen von Fahrzeugtypen sowie zur Reaktion darauf, und die Verfahren, mit denen bewertet wird, ob die implementierten Cybersicherheitsmaßnahmen angesichts neu ermittelter Cyberbedrohungen und Schwachstellen noch wirksam sind;

h) die Verfahren zur Bereitstellung einschlägiger Daten, die eine Analyse versuchter oder erfolgreicher Cyberangriffe unterstützen.

7.2.2.3. Der Fahrzeughersteller muss nachweisen, dass mit den Verfahren im Rahmen seines Cybersicherheitsmanagementsystems sichergestellt werden kann, dass ausgehend von einer Kategorisierung gemäß dem Absatz 7.2.2.2 Buchstabe c und Absatz 7.2.2.2 Buchstabe g Cyberbedrohungen und Schwachstellen, die eine Reaktion des Fahrzeugherstellers erforderlich machen, innerhalb eines angemessenen Zeitfensters gemindert werden.

7.2.2.4. Der Fahrzeughersteller muss nachweisen, dass mit den Verfahren im Rahmen seines Cybersicherheitsmanagementsystems sichergestellt werden kann, dass die in Absatz 7.2.2.2 Buchstabe g vorgesehene Überwachung ununterbrochen erfolgt. Dazu gehört:

a) die Einbeziehung von Fahrzeugen nach der Erstzulassung in die Überwachung;

b) die Fähigkeit, Cyberbedrohungen, Schwachstellen und Cyberangriffe anhand von Fahrzeugdaten und Fahrzeugprotokollen zu analysieren und zu erkennen. Dabei sind Absatz 1.3 und die Persönlichkeitsrechte von Fahrzeughaltern oder Fahrern, insbesondere was den Aspekt der Zustimmung angeht, zu beachten.

7.2.2.5. Der Fahrzeughersteller muss in Anbetracht der Vorschriften laut Absatz 7.2.2.2 darlegen, wie sein Cybersicherheitsmanagementsystem mit möglicherweise bestehenden wechselseitigen Abhängigkeiten mit Zulieferern, Dienstleistern oder Unterorganisationen des Herstellers umgeht.

7.3. Anforderungen an Fahrzeugtypen

7.3.1. Der Hersteller muss über eine gültige Konformitätsbescheinigung für das Cybersicherheitsmanagementsystem verfügen, das für den zu genehmigenden Fahrzeugtyp maßgeblich ist. Kann der Fahrzeughersteller jedoch für Typgenehmigungen von Fahrzeugen der Klassen M, N und O, die vor dem 1. Juli 2024 erteilt wurden, und für Typgenehmigungen von Fahrzeugen der Klasse L, die vor dem 1. Juli 2029 erteilt wurden, sowie für jede Erweiterung nachweisen, dass der Fahrzeugtyp nicht in Übereinstimmung mit dem CSMS entwickelt werden konnte, muss er nachweisen, dass in der Entwicklungsphase des betreffenden Fahrzeugtyps die Cybersicherheit angemessen berücksichtigt wurde.

7.3.2. Der Fahrzeughersteller muss für den zu genehmigenden Fahrzeugtyp die lieferantenbezogenen Risiken ermitteln und bewältigen.

7.3.3. Der Fahrzeughersteller muss die kritischen Elemente des Fahrzeugtyps ermitteln, eine erschöpfende Risikobewertung für den Fahrzeugtyp durchführen und mit den ermittelten Risiken angemessen umgehen bzw. sie bewältigen. Bei der Risikobewertung sind die einzelnen Elemente des Fahrzeugtyps und ihre Wechselwirkungen zu berücksichtigen. Bei der Risikobewertung sind ferner Wechselwirkungen mit sämtlichen externen Systemen zu berücksichtigen. Bei der Bewertung der Risiken muss der Fahrzeughersteller die Risiken im Zusammenhang mit allen in Anhang 5 Teil A genannten Bedrohungen sowie alle sonstigen einschlägigen Risiken berücksichtigen.

7.3.4. Der Fahrzeughersteller muss den Fahrzeugtyp gegen die in der Risikobewertung des Fahrzeugherstellers ermittelten Risiken schützen. Zum Schutz des Fahrzeugtyps sind angemessene Minderungsmaßnahmen vorzusehen. Diese umfassen alle in Anhang 5 Teil B und Teil C genannten, für die ermittelten Risiken relevanten Minderungsmaßnahmen. Wenn jedoch eine in Anhang 5 Teil B oder Teil C vorgesehene Minderungsmaßnahme für das ermittelte Risiko nicht relevant oder nicht ausreichend ist, muss der Fahrzeughersteller sicherstellen, dass eine andere, geeignete Maßnahme vorgesehen wird.

Insbesondere für Typgenehmigungen von Fahrzeugen der Klassen M, N und O, die vor dem 1. Juli 2024 erteilt wurden, und für Typgenehmigungen von Fahrzeugen der Klasse L, die vor dem 1. Juli 2029 erteilt wurden, sowie für jede Erweiterung muss der Fahrzeughersteller sicherstellen, dass eine andere, geeignete Minderungsmaßnahme vorgesehen wird, falls keine der in Anhang 5 Teil B oder C aufgeführte Minderungsmaßnahme technisch machbar ist. Die entsprechende Bewertung der technischen Durchführbarkeit muss der Hersteller der Genehmigungsbehörde vorlegen.

7.3.5. Der Fahrzeughersteller muss angemessene und verhältnismäßige Maßnahmen ergreifen, um bestimmte Umgebungen des Fahrzeugtyps (falls vorhanden) in Bezug auf die Speicherung und Ausführung von Software, Diensten, Anwendungen oder Daten des Anschlussmarktes zu sichern.

7.3.6. Der Fahrzeughersteller muss vor der Typgenehmigung angemessene und ausreichende Tests durchführen, um die Wirksamkeit der implementierten Sicherheitsmaßnahmen zu überprüfen.

7.3.7. Der Fahrzeughersteller muss für den Fahrzeugtyp Maßnahmen vorsehen, um

a) Cyberangriffe auf Fahrzeuge dieses Fahrzeugtyps zu erkennen und zu verhindern;

b) die Überwachungskapazitäten des Fahrzeugherstellers zur Erkennung von für den Fahrzeugtyp einschlägigen Bedrohungen, Schwachstellen und Cyberangriffen zu unterstützen;

c) Datenforensik bereitzustellen, um eine Analyse versuchter oder erfolgreicher Cyberangriffe zu ermöglichen.

7.3.8. Für die Zwecke dieser Regelung verwendete kryptografische Module müssen den einheitlichen Normen entsprechen. Entsprechen die verwendeten kryptografischen Module den einheitlichen Normen nicht, muss der Fahrzeughersteller ihre Verwendung begründen.

7.4. Bestimmungen zur Berichterstattung

7.4.1. Der Fahrzeughersteller muss der Genehmigungsbehörde oder dem technischen Dienst mindestens einmal jährlich, gegebenenfalls auch häufiger, über die Ergebnisse seiner Überwachungstätigkeiten gemäß Absatz 7.2.2.2 Buchstabe g Bericht erstatten; dazu gehören auch einschlägige Informationen zu neuen Cyberangriffen. Der Fahrzeughersteller muss der Genehmigungsbehörde oder dem technischen Dienst auch mitteilen und bestätigen, dass die für seine Fahrzeugtypen implementierten Maßnahmen zur Minderung von Cybersicherheitsrisiken weiterhin wirksam sind und alle zusätzlichen Maßnahmen ergriffen wurden.

7.4.2. Die Genehmigungsbehörde oder der technische Dienst muss die bereitgestellten Informationen überprüfen und, falls erforderlich, den Fahrzeughersteller auffordern, Abhilfe zu schaffen, wenn erkannt wurde, dass bestimmte Minderungsmaßnahmen nicht mehr wirksam sind.

Wenn die Meldung oder Antwort nicht ausreichend ist, kann die Genehmigungsbehörde beschließen, die Konformitätsbescheinigung für das CSMS gemäß Absatz 6.8 zurückzunehmen.

8. Änderung des Fahrzeugtyps und Erweiterung der Typgenehmigung

8.1. Die Genehmigungsbehörde, die den Fahrzeugtyp genehmigt hat, muss über jede Änderung des Fahrzeugtyps benachrichtigt werden, die sich auf die nach der vorliegenden Regelung erforderliche technische Leistung im Hinblick auf die Cybersicherheit und/oder auf die Dokumentation auswirkt. Die Genehmigungsbehörde kann dann

8.1.1. feststellen, dass die vorgenommenen Änderungen nach wie vor mit den Vorschriften und der Dokumentation der vorhandenen Typgenehmigung im Einklang stehen, oder

8.1.2. eine gemäß Absatz 5 erforderliche ergänzende Bewertung durchführen und gegebenenfalls einen weiteren Prüfbericht von dem technischen Dienst anfordern, der für die Durchführung der Tests zuständig ist.

8.1.3. Die Bestätigung, Erweiterung oder Versagung der Genehmigung ist unter Angabe der Änderungen mit einem Mitteilungsblatt mitzuteilen, das dem Muster in Anhang 2 dieser Regelung entspricht. Die Genehmigungsbehörde, die die Erweiterung der Genehmigung bescheinigt, teilt dieser Erweiterung eine laufende Nummer zu und unterrichtet hierüber die anderen Vertragsparteien des Übereinkommens von 1958, die diese Regelung anwenden, mit einem Mitteilungsblatt, das dem Muster in Anhang 2 dieser Regelung entspricht.

9. Übereinstimmung der Produktion

9.1. Die Verfahren zur Kontrolle der Übereinstimmung der Produktion müssen den in Anlage 1 zum Übereinkommen von 1958 (E/ECE/TRANS/505/Rev.3) beschriebenen Verfahren entsprechen, wobei folgende Vorschriften eingehalten sein müssen:

9.1.1. Der Inhaber einer Genehmigung muss sicherstellen, dass die Ergebnisse der Prüfungen der Übereinstimmung der Produktion protokolliert werden und die beigefügten Unterlagen während eines nach Absprache mit der Genehmigungsbehörde oder dem technischen Dienst festzulegenden Zeitraums verfügbar bleiben. Dieser Zeitraum darf, gerechnet von dem Zeitpunkt, an dem die Herstellung endgültig eingestellt wird, zehn Jahre nicht übersteigen.

9.1.2. Die Genehmigungsbehörde, die die Typgenehmigung erteilt hat, kann jederzeit die in jeder Fertigungsanlage angewandten Verfahren zur Kontrolle der Übereinstimmung der Produktion überprüfen. Diese Überprüfungen sind in der Regel einmal alle drei Jahre durchzuführen.

10. Maßnahmen bei Abweichungen der Produktion

10.1. Die für einen Fahrzeugtyp nach dieser Regelung erteilte Genehmigung kann zurückgenommen werden, wenn die Vorschriften dieser Regelung nicht eingehalten sind oder Prüffahrzeuge den Vorschriften dieser Regelung nicht entsprechen.

10.2. Nimmt eine Vertragspartei des Übereinkommens eine von ihr zuvor erteilte Genehmigung zurück, unterrichtet sie davon unverzüglich die anderen Vertragsparteien, die diese Regelung anwenden, mit einem Mitteilungsblatt, das dem Muster in Anhang 2 dieser Regelung entspricht.

11. Endgültige Einstellung der Produktion

11.1. Stellt der Inhaber einer Genehmigung die Produktion eines Fahrzeugtyps nach dieser Regelung endgültig ein, so hat er hierüber die Behörde, die die Genehmigung erteilt hat, zu unterrichten. Nach Erhalt der entsprechenden Mitteilung hat diese Behörde die anderen Vertragsparteien des Übereinkommens, die diese Regelung anwenden, hierüber mit einer Abschrift des Mitteilungsblatts der Genehmigung zu unterrichten, die am Schluss in Großbuchstaben den unterschriebenen und datierten Vermerk „PRODUKTION EINGESTELLT“ trägt.

12. Namen und Anschriften der technischen Dienste, die die Prüfungen für die Genehmigung durchführen, und der Typgenehmigungsbehörden

12.1. Die Vertragsparteien des Übereinkommens, die diese Regelung anwenden, teilen dem Sekretariat der Vereinten Nationen die Namen und Anschriften der technischen Dienste, die die Prüfungen für die Genehmigung durchführen, und der Typgenehmigungsbehörden, die Genehmigungen erteilen, denen die Mitteilungsblätter über in anderen Ländern erteilte, erweiterte, versagte oder zurückgenommene Genehmigungen zu übersenden sind, mit.

ANHANG 1

Beschreibungsbogen

Die nachstehenden Angaben sind, soweit sie infrage kommen, zusammen mit dem Verzeichnis der beiliegenden Unterlagen in dreifacher Ausfertigung einzureichen. Liegen Zeichnungen bei, so müssen diese das Format A4 haben oder auf das Format A4 gefaltet sein und hinreichende Einzelheiten in geeignetem Maßstab enthalten. Liegen Fotografien bei, so müssen diese hinreichende Einzelheiten erkennen lassen.

1. Marke (Handelsname des Herstellers): .....

2. Typ und Handelsbezeichnungen: .....

3. Merkmale zur Typenidentifizierung, falls am Fahrzeug vorhanden: .....

4. Lage dieser Kennzeichnung: .....

5. Fahrzeugklasse(n): .....

6. Name und Anschrift des Herstellers/Bevollmächtigten des Herstellers: .....

7. Namen und Anschriften der Fertigungsstätten .....

8. Fotos und/oder Zeichnungen eines repräsentativen Fahrzeugs: .....

9. Cybersicherheit

9.1. Allgemeine Baumerkmale des Fahrzeugtyps, darunter

a) die für die Cybersicherheit des Fahrzeugtyps maßgeblichen Fahrzeugsysteme;

b) die Bauteile der für die Cybersicherheit maßgeblichen Systeme;

c) die Interaktionen dieser Systeme mit anderen Systemen innerhalb des Fahrzeugtyps und mit externen Schnittstellen.

9.2. Schematische Darstellung des Fahrzeugtyps

9.3. Nummer der Konformitätsbescheinigung für das CSMS: .....

9.4. Unterlagen zu dem zu genehmigenden Fahrzeugtyp, aus denen die Ergebnisse der Risikobewertung und die ermittelten Risiken hervorgehen: .....

9.5. Unterlagen zu dem zu genehmigenden Fahrzeugtyp, aus denen hervorgeht, welche Minderungsmaßnahmen in den aufgeführten Systemen oder in Bezug auf den Fahrzeugtyp implementiert wurden und wie diese die festgestellten Risiken eindämmen: .....

9.6. Unterlagen zu dem zu genehmigenden Fahrzeugtyp, aus denen der Schutz bestimmter Umgebungen in Bezug auf Software, Dienste, Anwendungen oder Daten des Anschlussmarktes hervorgeht: .....

9.7. Unterlagen zu dem zu genehmigenden Fahrzeugtyp, aus denen die Art der durchgeführten Tests zur Überprüfung der Cybersicherheit des Fahrzeugtyps und seiner Systeme sowie die Ergebnisse dieser Tests hervorgehen: .....

9.8. Beschreibung der Lieferkette im Hinblick auf die Cybersicherheit: .....

Anhang 1 — Anlage 1

Muster der Konformitätserklärung des Herstellers für das CSMS

Erklärung des Herstellers über die Einhaltung der Anforderungen an das Cybersicherheitsmanagementsystem

Name des Herstellers: .....

Anschrift des Herstellers: .....

..... (*Name des Herstellers*)

bescheinigt, dass die zur Einhaltung der in Absatz 7.2 der UN-Regelung Nr. 155 festgelegten Anforderungen an das Cybersicherheitsmanagementsystem erforderlichen Verfahren vorhanden sind und regelmäßig überprüft werden.

Ausgestellt in: .....(*Ort*)

Datum: .....

Name des Unterzeichnenden: .....

Funktion des Unterzeichnenden: .....

(Stempel und Unterschrift des Bevollmächtigten des Herstellers)

ANHANG 2

Mitteilung

(größtes Format: A4 (210 mm × 297 mm))



ausgestellt von: Bezeichnung der Behörde:
.....
.....
.....

über die (2): Erteilung der Genehmigung
Erweiterung der Genehmigung
Rücknahme der Genehmigung mit Wirkung ab dem TT.MM.JJJJ
Versagung der Genehmigung
Endgültige Einstellung der Produktion

für einen Fahrzeugtyp, nach der UN-Regelung Nr. 155

Nummer der Genehmigung: .....

Nummer der Erweiterung der Genehmigung: .....

Grund für die Erweiterung: .....

1. Marke (Handelsname des Herstellers): .....

2. Typ und allgemeine übliche Beschreibung(en): .....

3. Merkmale zur Typenidentifizierung, falls am Fahrzeug vorhanden: .....

3.1. Anbringungsstelle dieser Kennzeichnung: .....

4. Fahrzeugklasse(n): .....

5. Name und Anschrift des Herstellers/Bevollmächtigten des Herstellers: .....

6. Name(n) und Anschrift(en) der Fertigungsstätte(n) .....

7. Nummer der Konformitätsbescheinigung für das Cybersicherheitsmanagementsystem: .....

8. Technischer Dienst, der für die Durchführung der Prüfungen zuständig ist: .....

9. Datum des Prüfberichts: .....

10. Nummer des Prüfberichts: .....

11. Anmerkungen: (falls vorhanden): .....

12. Ort: .....

(1) Kennzahl des Landes, das die Genehmigung erteilt/erweitert/versagt/zurückgenommen hat (siehe Genehmigungsvorschriften in der Regelung).
(2) Nichtzutreffendes streichen.

13. Datum: ……

14. Unterschrift: ……

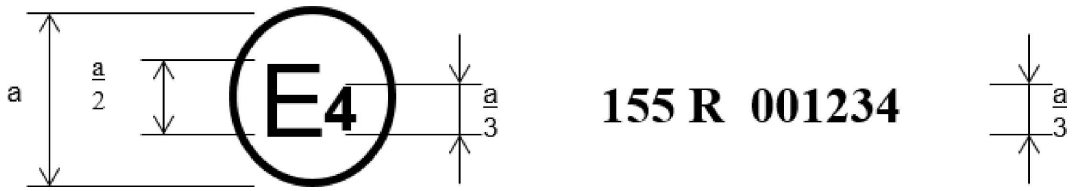
15. Das Inhaltsverzeichnis zu den bei der Genehmigungsbehörde hinterlegten Beschreibungsunterlagen, die auf Anforderung erhältlich sind, ist beigefügt:

ANHANG 3

Anordnung des Genehmigungszeichens

MUSTER A

(siehe Nummer 4.2 der vorliegenden Regelung)



a = min. 8 mm

Das oben dargestellte, an einem Fahrzeug angebrachte Genehmigungszeichen besagt, dass der betreffende Fahrzeugtyp in den Niederlanden (E4) nach der Regelung Nr. 155 unter der Genehmigungsnummer 001234 genehmigt worden ist. Aus den ersten beiden Ziffern der Genehmigungsnummer geht hervor, dass die Genehmigung nach den Vorschriften dieser Regelung in ihrer ursprünglichen Fassung (00) erteilt wurde.

ANHANG 4

MUSTER EINER KONFORMITÄTSBESCHEINIGUNG FÜR EIN CSMS

Bescheinigung der Übereinstimmung eines Cybersicherheitsmanagementsystems

mit der UN-Regelung Nr. 155

Nummer der Bescheinigung [*Referenznummer*]

[…… *Genehmigungsbehörde*]

bescheinigt, dass

Hersteller: ……

Anschrift des Herstellers: ……

mit den Vorschriften in Absatz 7.2 der Regelung Nr. 155 übereinstimmt.

Überprüfungen wurden durchgeführt am: ……

durch (Name und Anschrift der Genehmigungsbehörde oder des technischen Dienstes): ……

Nummer des Berichts: ……

Dieses Zertifikat ist gültig bis [……*Datum*]

Ort: […… *Ort*]

Datum: [……*Datum*]

[…… *Unterschrift*]

Anlagen: Beschreibung des Cybersicherheitsmanagementsystems durch den Hersteller.

ANHANG 5

Liste der Bedrohungen und der entsprechenden Minderungsmaßnahmen

1. Dieser Anhang umfasst drei Teile. In Teil A dieses Anhangs werden die Grundzüge der Bedrohungen, Schwachstellen und Angriffsmethoden beschrieben. In Teil B dieses Anhangs werden Minderungsmaßnahmen für die Bedrohungen beschrieben, die auf Fahrzeugtypen ausgerichtet sind. In Teil C werden Minderungsmaßnahmen für die Bedrohungen beschrieben, die auf Bereiche außerhalb von Fahrzeugen, z. B. IT-Back-Ends, abzielen.

2. Teil A, Teil B und Teil C müssen bei Risikobewertungen und Minderungsmaßnahmen, die von Fahrzeugherstellern vorzusehen sind, berücksichtigt werden.

3. Die übergeordneten Schwachstellen und entsprechende Beispiele wurden in Teil A indexiert. Diese Indexierung wurde auch in den Tabellen der Teile B und C übernommen, um die einzelnen Angriffsmethoden bzw. Schwachstellen mit einer Liste entsprechender Minderungsmaßnahmen zu verknüpfen.

4. Bei der Bedrohungsanalyse sind auch die möglichen Auswirkungen von Angriffen in Betracht zu ziehen. Dies kann dabei helfen, den Schweregrad eines Risikos zu bestimmen und zusätzliche Risiken zu ermitteln. Ein Angriff kann sich beispielsweise folgendermaßen auswirken:

   a) Beeinträchtigung des sicheren Betriebs eines Fahrzeugs;

   b) Ausfall von Fahrzeugfunktionen;

   c) Modifizierung der Software, veränderte Leistung;

   d) Änderung der Software, doch ohne Auswirkungen auf den Betrieb;

   e) Verletzung der Datensicherheit;

   f) Verletzung des Datengeheimnisses;

   g) Verlust der Verfügbarkeit von Daten;

   h) Sonstiges, einschließlich Kriminalität.

TEIL A

Schwachstellen bzw. Angriffsmethoden bezogen auf bestimmte Bedrohungen

Die übergeordneten Bedrohungen und die entsprechenden Schwachstellen bzw. Angriffsmethoden sind in Tabelle A1 aufgeführt.

Tabelle A1

Liste der Schwachstellen bzw. Angriffsmethoden bezogen auf die verschiedenen Bedrohungen

Übergeordnete und untergeordnete Schwachstelle/Bedrohung			Beispiel für die Schwachstelle bzw. Angriffsmethode	
4.3.1. Bedrohungen für Back-End-Server bezüglich Fahrzeugen auf der Straße	1	Backend-Server werden zum Angriff auf ein Fahrzeug oder zum Extrahieren von Daten genutzt	1.1	Missbrauch von Berechtigungen durch Personal (Insider-Angriff)
			1.2	Unbefugter Internetzugriff auf den Server (z. B. durch Backdoors, nicht gepatchte Systemsoftwareschwachstellen, SQL-Angriffe oder andere Mittel)
			1.3	Unbefugter physischer Zugriff auf den Server (z. B. mittels USB-Sticks oder anderer Datenträger, die sich mit dem Server verbinden)
	2	Backend-Serverdienste werden unterbrochen und der Fahrzeugbetrieb dadurch beeinträchtigt	2.1	Ein Angriff auf einen Backend-Server führt zu dessen Ausfall; dadurch wird z. B. die Interaktion mit Fahrzeugen und die Bereitstellung von Diensten, auf die diese angewiesen sind, verhindert

Übergeordnete und untergeordnete Schwachstelle/Bedrohung			Beispiel für die Schwachstelle bzw. Angriffsmethode	
	3	Verlust oder Gefährdung von Fahrzeugdaten auf Backend-Servern („Datenpanne“)	3.1	Missbrauch von Berechtigungen durch Personal (Insider-Angriff)
			3.2	Verlust von Informationen in der Cloud. Sensible Daten, die durch Drittanbieter von Cloud-Diensten gespeichert werden, können durch Angriffe oder Pannen verloren gehen
			3.3	Unbefugter Internetzugriff auf den Server (z. B. durch Backdoors, nicht gepatchte Systemsoftwareschwachstellen, SQL-Angriffe oder andere Mittel)
			3.4	Unbefugter physischer Zugriff auf den Server (z. B. mittels USB-Sticks oder anderer Medien, die sich mit dem Server verbinden)
			3.5	Informationssicherheitslücken durch unbeabsichtigte Weitergabe von Daten (z. B. durch Administratorfehler)
4.3.2 Bedrohungen für Fahrzeuge bezüglich ihrer Kommunikationskanäle	4	Spoofing von Nachrichten oder Daten, die vom Fahrzeug empfangen werden	4.1	Spoofing von Nachrichten durch Impersonation (z. B. kooperative Status- oder Fahrmanöverinformationen mittels V2X-Nachrichten, GNSS-Nachrichten usw.)
			4.2	Sybil-Attacke (um für andere Fahrzeuge vorzutäuschen, es seien viele Fahrzeuge auf der Straße)
	5	Kommunikationskanäle werden für die unerlaubte Manipulation, Löschung oder sonstige Änderung von Fahrzeugcode/-daten genutzt	5.1	Kommunikationskanäle ermöglichen Code-Injektion, z. B. können manipulierte Softwarebinärdateien in den Kommunikationsstrom injiziert werden
			5.2	Kommunikationskanäle ermöglichen die Manipulation von Fahrzeugdaten/-code
			5.3	Kommunikationskanäle ermöglichen das Überschreiben von Fahrzeugdaten/-code
			5.4	Kommunikationskanäle ermöglichen die Löschung von Fahrzeugdaten/-code
			5.5	Kommunikationskanäle ermöglichen die Einspeisung von Daten/Code in das Fahrzeug (Schreiben von Datencode)
	6	Kommunikationskanäle ermöglichen den Empfang nicht vertrauenswürdiger/ unzuverlässiger Nachrichten oder sind anfällig für Session Hijacking oder Replay-Angriffe	6.1	Akzeptieren von Informationen aus einer unzuverlässigen oder nicht vertrauenswürdigen Quelle
			6.2	Man-in-the-Middle-Angriff/Session Hijacking
			6.3	Replay-Angriff, z. B. ein Angriff auf ein Kommunikations-Gateway, der es dem Angreifer ermöglicht, die Software eines elektronischen Steuergeräts oder die Firmware des Gateways herabzustufen
	7	Informationen können leicht offengelegt werden, beispielsweise durch Abhören der Kommunikation oder die Ermöglichung des unbefugten Zugriffs auf sicherheitskritische Dateien oder Ordner	7.1	Abfangen von Informationen/Störstrahlung/ Überwachung der Kommunikation
			7.2	Erlangen von unbefugtem Zugriff auf Dateien oder Daten

Übergeordnete und untergeordnete Schwachstelle/Bedrohung			Beispiel für die Schwachstelle bzw. Angriffsmethode	
	8	Denial-of-Service-Attacken über Kommunikationskanäle zur Störung der Fahrzeugfunktionen	8.1	Das Fahrzeuginformationssystem wird gezielt mit so vielen Anfragen bombardiert, dass es die Aufgaben nicht mehr bewältigen kann
			8.2	Black-Hole-Angriff; um die Kommunikation zwischen Fahrzeugen zu stören, kann der Angreifer Nachrichten zwischen den Fahrzeugen blockieren
	9	Ein unprivilegierter Benutzer kann Sonderzugriffsrechte auf Fahrzeugsysteme erhalten	9.1	Ein unprivilegierter Benutzer kann Sonderzugriffsrechte erhalten, z. B. Root-Zugriff
	10	In Kommunikationsmedien eingebettete Viren können Fahrzeugsysteme infizieren	10.1	Ein in Kommunikationsmedien eingebetteter Virus infiziert Fahrzeugsysteme
	11	Vom Fahrzeug empfangene Nachrichten (z. B. X2V- oder Diagnosenachrichten) oder innerhalb des Fahrzeugs übertragene Nachrichten enthalten schädliche Inhalte	11.1	Schädliche interne Nachrichten (z. B. CAN-Nachrichten)
			11.2	Schädliche V2X-Nachrichten, z. B. Nachrichten zwischen Infrastruktur und Fahrzeug oder Nachrichten zwischen Fahrzeugen (z. B. CAM oder DENM)
			11.3	Schädliche Diagnosemeldungen
			11.4	Schädliche proprietäre Nachrichten (z. B. solche, die normalerweise vom OEM oder vom Lieferanten eines Bauteils, eines Systems oder einer Funktion gesendet werden)
4.3.3. Bedrohungen für Fahrzeuge bezüglich ihrer Aktualisierungsverfahren	12	Missbrauch oder Beeinträchtigung von Aktualisierungsverfahren	12.1	Beeinträchtigung von drahtlosen Softwareaktualisierungsverfahren; dazu gehört auch die Fälschung des Programms oder der Firmware zur Systemaktualisierung
			12.2	Beeinträchtigung von lokalen/physischen Softwareaktualisierungsverfahren; dazu gehört auch die Fälschung des Programms oder der Firmware zur Systemaktualisierung
			12.3	Die Software wird vor dem Aktualisierungsprozess manipuliert (und daher beschädigt), obwohl dieser intakt ist
			12.4	Beeinträchtigung von kryptografischen Schlüsseln des Softwareanbieters, um eine ungültige Aktualisierung zu ermöglichen
	13	Erwünschte Aktualisierungen können abgelehnt werden	13.1	Denial-of-Service-Attacke gegen den Aktualisierungsserver oder das Netzwerk, um wichtige Softwareaktualisierungen und/oder die Freigabe kundenspezifischer Funktionen zu verhindern
4.3.4. Bedrohungen für Fahrzeuge bezüglich unbeabsichtigter menschlicher Handlungen, die einen Cyberangriff begünstigen	15	Berechtigte Akteure können ohne ihr Wissen Maßnahmen durchführen, die einen Cyberangriff begünstigen	15.1	Ein unschuldiges Opfer (z. B. Eigentümer, Bediener oder Wartungstechniker) wird zu einer Aktion verleitet, mit der unbeabsichtigt Malware geladen oder ein Angriff ermöglicht wird
			15.2	Festgelegte Sicherheitsverfahren werden nicht befolgt

Übergeordnete und untergeordnete Schwachstelle/Bedrohung			Beispiel für die Schwachstelle bzw. Angriffsmethode	
4.3.5. Bedrohungen für Fahrzeuge bezüglich ihrer externen Vernetzung und Verbindungen	16	Ermöglichung eines Cyberangriffs durch Manipulation der Vernetzung von Fahrzeugfunktionen; dazu gehören Telematiksysteme, Fernsteuerungssysteme und Systeme, die drahtlose Kommunikation mit geringer Reichweite nutzen	16.1	Manipulation von Fernbedienungsfunktionen für Systeme wie Funkschlüssel, Wegfahrsperre und Ladestation
			16.2	Manipulation der Fahrzeugtelematik (z. B. Manipulation der Temperaturmessung empfindlicher Güter, ferngesteuertes Entriegeln von Frachttüren)
			16.3	Interferenzen mit drahtlosen Systemen oder Sensoren mit kurzer Reichweite
	17	Gehostete Software von Drittanbietern, z. B. Unterhaltungsanwendungen, die zum Angriff auf Fahrzeugsysteme genutzt werden	17.1	Manipulierte oder unsichere Anwendungen, die zum Angriff auf Fahrzeugsysteme genutzt werden
	18	Mit externen Schnittstellen, z. B. USB- oder OBD-Anschlüssen, verbundene Geräte, die zum Angriff auf Fahrzeugsysteme genutzt werden	18.1	Externe Schnittstellen wie USB-Anschlüsse oder andere als Angriffspunkte genutzte Anschlüsse, z. B. für Code-Injektion
			18.2	Mit einem Virus infizierte Datenträger werden an ein Fahrzeugsystem angeschlossen
			18.3	Ein Diagnosezugang (z. B. Dongles am OBD-Anschluss) wird zur Begünstigung eines Angriffs genutzt, z. B. durch Manipulation von Fahrzeugparametern (direkt oder indirekt)
4.3.6. Bedrohungen für Fahrzeugdaten/-code	19	Extraktion von Fahrzeugdaten/-code	19.1	Extraktion von urheberrechtlich geschützter oder proprietärer Software aus Fahrzeugsystemen (Produktpiraterie)
			19.2	Unbefugter Zugriff auf die personenbezogenen Daten des Eigentümers wie persönliche Identität, Kontodaten, Adressbuchdaten, Standortdaten, elektronische Fahrzeugkennung usw.
			19.3	Extraktion kryptografischer Schlüssel
	20	Manipulation von Fahrzeugdaten/-code	20.1	Illegale/unbefugte Änderungen der elektronischen Fahrzeugkennung
			20.2	Identitätsbetrug, z. B. wenn ein Nutzer bei der Kommunikation mit Mautsystemen eine andere Identität anzeigt, Hersteller-Back-End
			20.3	Aktionen zur Umgehung von Überwachungssystemen (z. B. Hacking/ Manipulation/Blockierung von Nachrichten wie ODR-Tracker-Daten oder Anzahl der Fahrten)
			20.4	Datenmanipulation zur Fälschung der Fahrdaten des Fahrzeugs (z. B. Kilometerstand, Fahrgeschwindigkeit, Fahrtrichtung usw.)
			20.5	Unbefugte Änderungen von Systemdiagnosedaten
	21	Löschung von Daten/Code	21.1	Unbefugtes Löschen/Manipulieren von Systemereignisprotokollen
	22	Einspeisung von Malware	22.2	Einspeisung von Schadsoftware oder Schadsoftwareaktivitäten

Übergeordnete und untergeordnete Schwachstelle/Bedrohung			Beispiel für die Schwachstelle bzw. Angriffsmethode	
	23	Einspeisung neuer Software oder Überschreiben vorhandener Software	23.1	Fälschung der Software des Fahrzeugsteuerungs- oder -informationssystems
	24	Störung von Systemen oder Vorgängen	24.1	Denial-of-Service-Attacken, die im internen Netzwerk z. B. durch Überlastung eines CAN-Busses oder durch Provozieren von Störungen an einem elektronischen Steuergerät aufgrund großer Nachrichtenmengen ausgelöst werden kann
	25	Manipulation von Fahrzeugparametern	25.1	Unbefugter Zugriff zur Verfälschung der Konfigurationsparameter von Schlüsselfunktionen des Fahrzeugs, wie z. B. Bremsdaten, Airbag-Auslöseschwelle usw.
			25.2	Unbefugter Zugriff zur Verfälschung der Ladeparameter, z. B. Ladespannung, Ladeleistung, Batterietemperatur usw.
4.3.7. Potenzielle Schwachstellen, die ausgenutzt werden könnten, wenn Schutz oder Härtung nicht ausreichen	26	Kryptografische Technologien können beeinträchtigt werden oder werden unzureichend angewendet	26.1	Eine Kombination aus kurzen Verschlüsselungscodes und langen Gültigkeitszeiträumen ermöglicht es dem Angreifer, die Verschlüsselung zu knacken
			26.2	Unzureichender Einsatz kryptografischer Algorithmen zum Schutz sensibler Systeme
			26.3	Verwendung kryptografischer Algorithmen, die bereits veraltet sind oder es bald sein werden
	27	Teile oder Zubehör könnten beeinträchtigt werden, um Angriffe auf Fahrzeuge zu ermöglichen	27.1	Hardware oder Software, die entwickelt wurde, um einen Angriff zu ermöglichen, oder die so konzipiert ist, dass sie die Kriterien zur Beendigung eines Angriffs nicht erfüllt
	28	Software- oder Hardwareentwicklung führt zu Schwachstellen	28.1	Softwarefehler. Vorhandene Softwarefehler können die Grundlage für potenzielle, nutzbare Schwachstellen bilden. Dies trifft insbesondere dann zu, wenn die Software nicht getestet wurde, um bekannten, fehlerhaften Code bzw. Programmfehler zu finden bzw. das Risiko von unbekanntem, fehlerhaftem Code bzw. Programmfehlern zu verringern
			28.2	Überbleibsel aus der Entwicklungsphase (z. B. Debug-Ports, JTAG-Ports, Mikroprozessoren, Entwicklungszertifikate, Entwicklerpasswörter usw.) können Angreifern ermöglichen, auf elektronische Steuergeräte zuzugreifen oder sich höhere Berechtigungen zu verschaffen
	29	Entstehen von Schwachstellen durch das Netzwerkdesign	29.1	Nicht genutzte, offen gelassene Ports bieten Zugang zu Netzwerksystemen
			29.2	Umgehung der Netzwerktrennung, um Kontrolle zu erlangen. Ein spezifisches Beispiel ist die Nutzung ungeschützter Gateways oder Zugangspunkte (wie z. B. LKW-Anhänger-Gateways), um Schutzmaßnahmen zu umgehen und Zugang zu anderen Netzwerksegmenten zu erhalten und schädliche Aktionen durchzuführen, wie z. B. willkürliche CAN-Bus-Nachrichten zu senden
	31	Mögliche unbeabsichtigte Übertragung von Daten	31.1	Informationssicherheitslücken. Personenbezogene Daten können bei einem Wechsel des Fahrzeugnutzers (z. B. durch Verkauf oder Neuvermietung) in die falschen Hände geraten

Übergeordnete und untergeordnete Schwachstelle/Bedrohung			Beispiel für die Schwachstelle bzw. Angriffsmethode	
	32	Ermöglichung eines Angriffs durch physische Manipulation eines Systems	32.1	Manipulation elektronischer Hardware, z. B. wenn in einem Fahrzeug unzulässige elektronische Hardware hinzugefügt wird, um einen Man-in-the-Middle-Angriff zu ermöglichen Austausch zulässiger elektronischer Hardware (z. B. Sensoren) durch unzulässige elektronische Hardware Manipulation der von einem Sensor erfassten Daten (z. B. wenn mittels eines Magneten der am Getriebe angebrachte Hall-Sensor manipuliert wird)

TEIL B

Minderungsmaßnahmen für Bedrohungen, die auf Fahrzeuge ausgerichtet sind

1. Minderungsmaßnahmen für Fahrzeugkommunikationskanäle

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Fahrzeugkommunikationskanälen sind in Tabelle B1 aufgeführt.

Tabelle B1

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Fahrzeugkommunikationskanälen

Referenz Tabelle A1	Bedrohungen für Fahrzeugkommunikationskanäle	Ref.	Minderungsmaßnahme
4.1	Spoofing von Nachrichten durch Impersonation (z. B. kooperative Status- oder Fahrmanöverinformationen über V2X-Nachrichten, GNSS-Nachrichten usw.)	M10	Das Fahrzeug muss die Authentizität und Integrität der empfangenen Nachrichten überprüfen
4.2	Sybil-Attacke (um für andere Fahrzeuge vorzutäuschen, es seien viele Fahrzeuge auf der Straße)	M11	Es sind Sicherheitsmaßnahmen zur Speicherung kryptografischer Schlüssel vorzusehen (z. B. Verwendung von Hardwaresicherheitsmodulen)
5.1	Kommunikationskanäle ermöglichen Code-Injektion in Fahrzeugdaten/-code, z. B. können manipulierte Softwarebinärdateien in den Kommunikationsstrom injiziert werden	M10 M6	Das Fahrzeug muss die Authentizität und Integrität der empfangenen Nachrichten überprüfen Bereits bei der Konzeption der Systeme müssen Sicherheitsvorkehrungen vorgesehen werden, um Risiken zu minimieren
5.2	Kommunikationskanäle ermöglichen die Manipulation von Fahrzeugdaten/-code	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden
5.3	Kommunikationskanäle ermöglichen das Überschreiben von Fahrzeugdaten/-code		
5.4 21.1	Kommunikationskanäle ermöglichen die Löschung von Fahrzeugdaten/-code		
5.5	Kommunikationskanäle ermöglichen die Einspeisung von Daten/Code in Fahrzeugsysteme (Schreiben von Datencode)		

Referenz Tabelle A1	Bedrohungen für Fahrzeugkommunikationskanäle	Ref.	Minderungsmaßnahme
6.1	Akzeptieren von Informationen aus einer unzuverlässigen oder nicht vertrauenswürdigen Quelle	M10	Das Fahrzeug muss die Authentizität und Integrität der empfangenen Nachrichten überprüfen
6.2	Man-in-the-Middle-Angriff/Session Hijacking	M10	Das Fahrzeug muss die Authentizität und Integrität der empfangenen Nachrichten überprüfen
6.3	Replay-Angriff, z. B. ein Angriff auf ein Kommunikations-Gateway, der es dem Angreifer ermöglicht, die Software eines elektronischen Steuergeräts oder die Firmware des Gateways herabzustufen		
7.1	Abfangen von Informationen/ Störstrahlung/Überwachung der Kommunikation	M12	Vertrauliche Daten, die an das Fahrzeug oder vom Fahrzeug übermittelt werden, müssen geschützt werden
7.2	Erlangen von unbefugtem Zugriff auf Dateien oder Daten	M8	Das Systemdesign und die Zugangskontrolle müssen so ausgelegt sein, dass Unbefugte nicht auf personenbezogene oder systemkritische Daten zugreifen können. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
8.1	Das Fahrzeuginformationssystem wird gezielt mit so vielen Anfragen bombardiert, dass es die Aufgaben nicht mehr bewältigen kann	M13	Es sind Maßnahmen zur Erkennung und Behebung einer Denial-of-Service-Attacke zu treffen
8.2	Black-Hole-Angriff, Störung der Kommunikation zwischen Fahrzeugen durch Blockieren der Übermittlung von Nachrichten an andere Fahrzeuge	M13	Es sind Maßnahmen zur Erkennung und Behebung einer Denial-of-Service-Attacke zu treffen
9.1	Ein unprivilegierter Benutzer kann Sonderzugriffsrechte erhalten, z. B. Root-Zugriff	M9	Es sind Maßnahmen zur Verhinderung und Erkennung von unbefugtem Zugriff zu treffen
10.1	Ein in Kommunikationsmedien eingebetteter Virus infiziert Fahrzeugsysteme	M14	Maßnahmen zum Schutz von Systemen gegen eingebettete Viren/Malware sind zu erwägen
11.1	Schädliche interne Nachrichten (z. B. CAN-Nachrichten)	M15	Maßnahmen zur Erkennung schädlicher interner Nachrichten oder Aktivitäten sind zu erwägen
11.2	Schädliche V2X-Nachrichten, z. B. Nachrichten zwischen Infrastruktur und Fahrzeug oder Nachrichten zwischen Fahrzeugen (z. B. CAM oder DENM)	M10	Das Fahrzeug muss die Authentizität und Integrität der empfangenen Nachrichten überprüfen
11.3	Schädliche Diagnosemeldungen		
11.4	Schädliche proprietäre Nachrichten (z. B. solche, die normalerweise vom OEM oder vom Lieferanten eines Bauteils, eines Systems oder einer Funktion gesendet werden)		

2. Minderungsmaßnahmen für den Aktualisierungsprozess

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit dem Aktualisierungsprozess sind in Tabelle B2 aufgeführt.

Tabelle B2

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit dem Aktualisierungsprozess

Referenz Tabelle A1	Bedrohungen für den Aktualisierungsprozess	Ref.	Minderungsmaßnahme
12.1	Beeinträchtigung von drahtlosen Softwareaktualisierungsverfahren; dazu gehört auch die Fälschung des Programms oder der Firmware zur Systemaktualisierung	M16	Es sind sichere Softwareaktualisierungsverfahren anzuwenden
12.2	Beeinträchtigung von lokalen/physischen Softwareaktualisierungsverfahren; dazu gehört auch die Fälschung des Programms oder der Firmware zur Systemaktualisierung		
12.3	Die Software wird vor dem Aktualisierungsprozess manipuliert (und daher beschädigt), obwohl dieser intakt ist		
12.4	Beeinträchtigung von kryptografischen Schlüsseln des Softwareanbieters, um eine ungültige Aktualisierung zu ermöglichen	M11	Es sind Sicherheitsmaßnahmen zur Speicherung kryptografischer Schlüssel vorzusehen
13.1	Denial-of-Service-Attacke gegen den Aktualisierungsserver oder das Netzwerk, um wichtige Softwareaktualisierungen und/oder die Freigabe kundenspezifischer Funktionen zu verhindern	M3	An Back-End-Systemen sind Sicherheitsmaßnahmen anzuwenden. Wenn Back-End-Server unabdingbar für die Bereitstellung von Diensten sind, sind Wiederherstellungsmaßnahmen für den Fall von Systemausfällen vorzusehen. Beispiele für Sicherheitsmaßnahmen bietet das OWASP

3. Minderungsmaßnahmen bezüglich unbeabsichtigter menschlicher Handlungen, die einen Cyberangriff begünstigen

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen, die einen Cyberangriff begünstigen, sind in Tabelle B3 aufgeführt.

Tabelle B3

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen, die einen Cyberangriff begünstigen

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen	Ref.	Minderungsmaßnahme
15.1	Ein unschuldiges Opfer (z. B. Eigentümer, Bediener oder Wartungstechniker) wird zu einer Aktion verleitet, mit der unbeabsichtigt Malware geladen oder ein Angriff ermöglicht wird	M18	Es sind Maßnahmen zur Festlegung und Kontrolle von Nutzerrollen und Zugriffsrechten nach dem Least-Privilege-Prinzip vorzusehen

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen	Ref.	Minderungsmaßnahme
15.2	Festgelegte Sicherheitsverfahren werden nicht befolgt	M19	Die Organisationen sorgen dafür, dass Sicherheitsverfahren festgelegt und befolgt werden, einschließlich der Protokollierung von Operationen und des Zugriffs im Zusammenhang mit der Verwaltung der Sicherheitsfunktionen

4. Minderungsmaßnahmen bezüglich externer Vernetzung und Verbindungen

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit externer Vernetzung und Verbindungen sind in Tabelle B4 aufgeführt.

Tabelle B4

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit externer Vernetzung und Verbindungen

Referenz Tabelle A1	Bedrohungen für externe Vernetzung und Verbindungen	Ref.	Minderungsmaßnahme
16.1	Manipulation von Fernbedienungsfunktionen für Fahrzeugsysteme wie Funkschlüssel, Wegfahrsperre und Ladestation	M20	Bei Systemen mit Fernzugriff sind Sicherheitsmaßnahmen anzuwenden.
16.2	Manipulation der Fahrzeugtelematik (z. B. Manipulation der Temperaturmessung empfindlicher Güter, ferngesteuertes Entriegeln von Frachttüren)		
16.3	Interferenzen mit drahtlosen Systemen oder Sensoren mit kurzer Reichweite		
17.1	Manipulierte oder unsichere Anwendungen, die zum Angriff auf Fahrzeugsysteme genutzt werden	M21	Software muss sicherheitsüberprüft, authentifiziert und integritätsgeschützt sein. Es sind Sicherheitsmaßnahmen anzuwenden, um das Risiko durch Software Dritter zu begrenzen, die dazu bestimmt ist oder bei der vorauszusehen ist, dass sie im Fahrzeug untergebracht wird
18.1	Externe Schnittstellen wie USB-Anschlüsse oder andere als Angriffspunkte genutzte Anschlüsse, z. B. für Code-Injektion	M22	An externen Schnittstellen sind Sicherheitsmaßnahmen anzuwenden
18.2	Mit einem Virus infizierte Datenträger werden an das Fahrzeug angeschlossen		
18.3	Ein Diagnosezugang (z. B. Dongles am OBD-Anschluss) wird zur Begünstigung eines Angriffs genutzt, z. B. durch Manipulation von Fahrzeugparametern (direkt oder indirekt)	M22	An externen Schnittstellen sind Sicherheitsmaßnahmen anzuwenden

5. Minderungsmaßnahmen bezüglich potenzieller Ziele oder Motivationen für einen Angriff

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit potenziellen Zielen oder Motivationen für einen Angriff sind in Tabelle B5 aufgeführt.

Tabelle B5

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit potenziellen Zielen oder Motivationen für einen Angriff

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit potenziellen Zielen oder Motivationen für einen Angriff	Ref.	Minderungsmaßnahme
19.1	Extraktion von urheberrechtlich geschützter oder proprietärer Software aus Fahrzeugsystemen (Produktpiraterie/ Softwarediebstahl)	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
19.2	Unbefugter Zugriff auf die personenbezogenen Daten des Eigentümers wie persönliche Identität, Kontodaten, Adressbuchdaten, Standortdaten, elektronische Fahrzeugkennung usw.	M8	Das Systemdesign und die Zugangskontrolle müssen so ausgelegt sein, dass Unbefugte nicht auf personenbezogene oder systemkritische Daten zugreifen können. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
19.3	Extraktion kryptografischer Schlüssel	M11	Es sind Sicherheitsmaßnahmen zur Speicherung kryptografischer Schlüssel vorzusehen, z. B. Sicherheitsmodule
20.1	Illegale/unbefugte Änderungen der elektronischen Fahrzeugkennung	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
20.2	Identitätsbetrug, z. B. wenn ein Nutzer bei der Kommunikation mit Mautsystemen eine andere Identität anzeigt, Hersteller-Back-End		
20.3	Aktionen zur Umgehung von Überwachungssystemen (z. B. Hacking/ Manipulation/Blockierung von Nachrichten wie ODR-Tracker-Daten oder Anzahl der Fahrten)	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden. Beispiele für Sicherheitsmaßnahmen bietet das OWASP Datenmanipulationsangriffe auf Sensoren oder übertragene Daten könnten durch Korrelieren der Daten aus verschiedenen Informationsquellen abgeschwächt werden
20.4	Datenmanipulation zur Fälschung der Fahrdaten des Fahrzeugs (z. B. Kilometerstand, Fahrgeschwindigkeit, Fahrtrichtung usw.)		
20.5	Unbefugte Änderungen von Systemdiagnosedaten		
21.1	Unbefugtes Löschen/Manipulieren von Systemereignisprotokollen	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
22.2	Einspeisung von Schadsoftware oder Schadsoftwareaktivitäten	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
23.1	Fälschung der Software des Fahrzeugsteuerungs- oder -informationssystems		

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit potenziellen Zielen oder Motivationen für einen Angriff	Ref.	Minderungsmaßnahme
24.1	Denial-of-Service-Attacken, die im internen Netzwerk z. B. durch Überlastung eines CAN-Busses oder durch Provozieren von Störungen an einem elektronischen Steuergerät aufgrund großer Nachrichtenmengen ausgelöst werden kann	M13	Es sind Maßnahmen zur Erkennung und Behebung einer Denial-of-Service-Attacke zu treffen
25.1	Unbefugter Zugriff zur Verfälschung der Konfigurationsparameter von Schlüsselfunktionen des Fahrzeugs, wie z. B. Bremsdaten, Airbag-Auslöseschwelle usw.	M7	Zum Schutz von Systemdaten/-code sind Zugriffskontrolltechniken und -konzepte anzuwenden. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
25.2	Unbefugter Zugriff zur Verfälschung der Ladeparameter, z. B. Ladespannung, Ladeleistung, Batterietemperatur usw.		

6. Minderungsmaßnahmen bezüglich potenzieller Schwachstellen, die ausgenutzt werden könnten, wenn Schutz oder Härtung nicht ausreichen

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit potenziellen Schwachstellen, die ausgenutzt werden könnten, wenn Schutz oder Härtung nicht ausreichen, sind in Tabelle B6 aufgeführt.

Tabelle B6

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit potenziellen Schwachstellen, die ausgenutzt werden könnten, wenn Schutz oder Härtung nicht ausreichen

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit potenziellen Schwachstellen, die ausgenutzt werden könnten, wenn Schutz oder Härtung nicht ausreichen	Ref.	Minderungsmaßnahme
26.1	Eine Kombination aus kurzen Verschlüsselungscodes und langen Gültigkeitszeiträumen ermöglicht es dem Angreifer, die Verschlüsselung zu knacken	M23	Bewährte Verfahren für die Cybersicherheit bei der Software- und Hardwareentwicklung sind zu befolgen
26.2	Unzureichender Einsatz kryptografischer Algorithmen zum Schutz sensibler Systeme		
26.3	Verwendung veralteter kryptografischer Algorithmen		
27.1	Hardware oder Software, die entwickelt wurde, um einen Angriff zu ermöglichen, oder die so konzipiert ist, dass sie die Kriterien zur Beendigung eines Angriffs nicht erfüllt	M23	Bewährte Verfahren für die Cybersicherheit bei der Software- und Hardwareentwicklung sind zu befolgen
28.1	Vorhandene Softwarefehler können die Grundlage für potenzielle, nutzbare Schwachstellen bilden. Dies trifft insbesondere dann zu, wenn die Software nicht getestet wurde, um bekannten, fehlerhaften Code bzw. Programmfehler zu finden bzw. das Risiko von unbekanntem, fehlerhaftem Code bzw. Programmfehlern zu verringern	M23	Bewährte Verfahren für die Cybersicherheit bei der Software- und Hardwareentwicklung sind zu befolgen Cybersicherheitstests mit angemessener Abdeckung

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit potenziellen Schwachstellen, die ausgenutzt werden könnten, wenn Schutz oder Härtung nicht ausreichen	Ref.	Minderungsmaßnahme
28.2	Überbleibsel aus der Entwicklungsphase (z. B. Debug-Ports, JTAG-Ports, Mikroprozessoren, Entwicklungszertifikate, Entwicklerpasswörter usw.) können es einem Angreifer ermöglichen, auf elektronische Steuergeräte zuzugreifen oder sich höhere Berechtigungen zu verschaffen		
29.1	Überflüssige, offen gelassene Ports bieten Zugang zu Netzwerksystemen		
29.2	Umgehung der Netzwerktrennung, um Kontrolle zu erlangen. Ein spezifisches Beispiel ist die Nutzung ungeschützter Gateways oder Zugangspunkte (wie z. B. LKW-Anhänger-Gateways), um Schutzmaßnahmen zu umgehen und Zugang zu anderen Netzwerksegmenten zu erhalten und schädliche Aktionen durchzuführen, wie z. B. willkürliche CAN-Bus-Nachrichten zu senden	M23	Bewährte Verfahren für die Cybersicherheit bei der Software- und Hardwareentwicklung sind zu befolgen Bewährte Verfahren für die Cybersicherheit bei Systemdesign und Systemintegration sind zu befolgen

7. Minderungsmaßnahmen bezüglich Datenverlusten/Datenpannen des Fahrzeugs

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Datenverlusten/Datenpannen des Fahrzeugs sind in Tabelle B7 aufgeführt.

Tabelle B7

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Datenverlusten/Datenpannen des Fahrzeugs

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit Datenverlusten/ Datenpannen des Fahrzeugs	Ref.	Minderungsmaßnahme
31.1	Informationssicherheitslücken. Der Schutz personenbezogener Daten kann bei einem Wechsel des Fahrzeugnutzers (z. B. durch Verkauf oder Neuvermietung) verletzt werden	M24	Bei der Speicherung personenbezogener Daten sind bewährte Verfahren zum Schutz der Datenintegrität und -vertraulichkeit zu befolgen.

8. Minderungsmaßnahmen bezüglich der Ermöglichung eines Angriffs durch physische Manipulation eines Systems

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit der Ermöglichung eines Angriffs durch physische Manipulation eines Systems sind in Tabelle B8 aufgeführt.

Tabelle B8

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit der Ermöglichung eines Angriffs durch physische Manipulation eines Systems

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit der Ermöglichung eines Angriffs durch physische Manipulation eines Systems	Ref.	Minderungsmaßnahme
32.1	Manipulation von OEM-Hardware, z. B. Hinzufügen unzulässiger Hardware in einem Fahrzeug, um einen Man-in-the-Middle-Angriff zu ermöglichen	M9	Es sind Maßnahmen zur Verhinderung und Erkennung von unbefugtem Zugriff zu treffen

TEIL C

Minderungsmaßnahmen für die Bedrohungen, die auf Bereiche außerhalb von Fahrzeugen abzielen

1. Minderungsmaßnahmen für Back-End-Server

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Back-End-Servern sind in Tabelle C1 aufgeführt.

Tabelle C1

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit Back-End-Servern

Referenz Tabelle A1	Bedrohungen für Back-End-Server	Ref.	Minderungsmaßnahme
1.1 & 3.1	Missbrauch von Berechtigungen durch Personal (Insider-Angriff)	M1	Auf Back-End-Systemen werden Sicherheitsmaßnahmen angewendet, um das Risiko eines Insider-Angriffs zu minimieren
1.2 & 3.3	Unbefugter Internetzugriff auf den Server (z. B. durch Backdoors, nicht gepatchte Systemsoftwareschwachstellen, SQL-Angriffe oder andere Mittel)	M2	Auf Back-End-Systemen werden Sicherheitsmaßnahmen angewendet, um den unbefugten Zugriff zu minimieren. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
1.3 & 3.4	Unbefugter physischer Zugriff auf den Server (z. B. mittels USB-Sticks oder anderer Datenträger, die sich mit dem Server verbinden)	M8	Das Systemdesign und die Zugangskontrolle müssen so ausgelegt sein, dass Unbefugte nicht auf personenbezogene oder systemkritische Daten zugreifen können
2.1	Ein Angriff auf einen Backend-Server führt zu dessen Ausfall; dadurch wird z. B. die Interaktion mit Fahrzeugen und die Bereitstellung von Diensten, auf die diese angewiesen sind, verhindert	M3	An Back-End-Systemen sind Sicherheitsmaßnahmen anzuwenden. Wenn Back-End-Server unabdingbar für die Bereitstellung von Diensten sind, sind Wiederherstellungsmaßnahmen für den Fall von Systemausfällen vorzusehen. Beispiele für Sicherheitsmaßnahmen bietet das OWASP
3.2	Verlust von Informationen in der Cloud. Sensible Daten, die durch Drittanbieter von Cloud-Diensten gespeichert werden, können durch Angriffe oder Pannen verloren gehen	M4	Es werden Sicherheitsmaßnahmen angewendet, um mit dem Cloud-Computing verbundene Risiken zu minimieren. Beispiele für Sicherheitsmaßnahmen bieten das OWASP und der Leitfaden für Cloud-Sicherheit (Cloud Security Guidance) der britischen NCSC
3.5	Informationssicherheitslücken durch unbeabsichtigte Weitergabe von Daten (z. B. durch Administratorfehler, Serveraufstellung in Garagen)	M5	Auf Back-End-Systemen werden Sicherheitsmaßnahmen angewendet, um Datenpannen zu verhindern. Beispiele für Sicherheitsmaßnahmen bietet das OWASP

2. Minderungsmaßnahmen bezüglich unbeabsichtigter menschlicher Handlungen

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen sind in Tabelle C2 aufgeführt.

Tabelle C2

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit unbeabsichtigten menschlichen Handlungen	Ref.	Minderungsmaßnahme
15.1	Ein unschuldiges Opfer (z. B. Eigentümer, Bediener oder Wartungstechniker) wird zu einer Aktion verleitet, mit der unbeabsichtigt Malware geladen oder ein Angriff ermöglicht wird	M18	Es sind Maßnahmen zur Festlegung und Kontrolle von Nutzerrollen und Zugriffsrechten nach dem Least-Privilege-Prinzip vorzusehen
15.2	Festgelegte Sicherheitsverfahren werden nicht befolgt	M19	Die Organisationen sorgen dafür, dass Sicherheitsverfahren festgelegt und befolgt werden, einschließlich der Protokollierung von Operationen und des Zugriffs im Zusammenhang mit der Verwaltung der Sicherheitsfunktionen

3. Minderungsmaßnahmen bezüglich physischer Datenverluste

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit physischen Datenverlusten sind in Tabelle C3 aufgeführt.

Tabelle C3

Minderungsmaßnahmen für Bedrohungen im Zusammenhang mit physischen Datenverlusten

Referenz Tabelle A1	Bedrohungen im Zusammenhang mit physischen Datenverlusten	Ref.	Minderungsmaßnahme
30.1	Verursachung von Schäden durch Dritte. Durch physische Schäden, die etwa bei Verkehrsunfällen oder Diebstahl entstehen, können sensible Daten verloren gehen oder beeinträchtigt werden	M24	Bei der Speicherung personenbezogener Daten sind bewährte Verfahren zum Schutz der Datenintegrität und -vertraulichkeit zu befolgen. Beispiele für Sicherheitsmaßnahmen bietet das ISO/SC27/WG5
30.2	Verluste durch DRM-Konflikte (Digital Right Management, digitale Rechteverwaltung). Benutzerdaten können aufgrund von DRM-Problemen gelöscht werden		
30.3	Sensible Daten bzw. deren Integrität können durch Abnutzung von IT-Komponenten verloren gehen, was zu kaskadierenden Problemen führen kann (z. B. bei Schlüsseländerungen)		