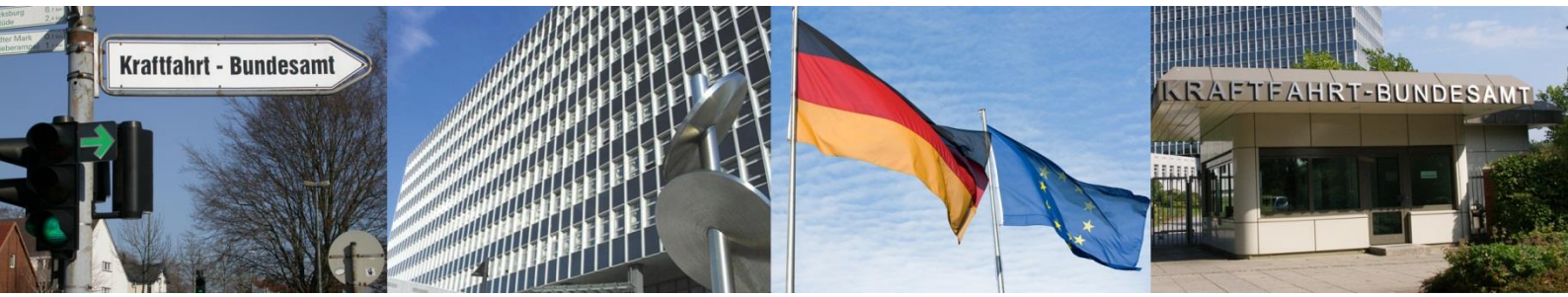
Kraftfahrt-
Bundesamt

Anwendung der Regeln für die Benennung/Anerkennung von Technischen Diensten (Kategorien A, B, D)

zu Prüfungen im Rahmen des

KBA-Typgenehmigungsverfahrens nach den UN-Regelungen 155/156

Stand: Januar 2021



Inhaltsverzeichnis

1 Einleitung

Dieses Dokument ergänzt die Festlegungen der Regeln für die Benennung/Anerkennung von Technischen Diensten (Kategorien A, B, D)[1]. Es ist insofern mitgeltend zu den Benennungsregeln des KBA und damit für alle in diesem Scope tätigen vom KBA benannten Technischen Dienste (TD) verbindlich[2].

Das Dokument wird entsprechend eventueller Hinweise der zuständigen UN- bzw. EU-Gremien und vorliegender Erfahrungen nach Konsultation des Arbeitskreises Technik (AK-T) bzw. seiner Arbeitsgruppe Cybersecurity (CS) überarbeitet. Die jeweils aktuelle Fassung wird im Technik-Portal der KBA-Homepage veröffentlicht

Das jeweils aktuelle Interpretation Document der UNECE zu UN-Regelungen ist zu beachten.

Das KBA kann Ausnahmen genehmigen. Entsprechende Anträge sind nach Möglichkeit rechtzeitig im Vorfeld zu stellen.

2 Verantwortlichkeiten

Das KBA

- benennt die TD nach seinen Benennungsregeln und diesem Dokument
- stellt das in den UN-R geforderte Zertifikat auf der Grundlage der Auditberichte und sonstigen Informationen aus, setzt dieses ggf. aus oder entzieht es
- erteilt die Typgenehmigung
- organisiert den Erfahrungsaustausch zwischen allen interessierten Parteien mit dem Ziel der Weiterentwicklung des Verfahrens
- ist zuständig für die Kommunikation mit den entsprechenden UN- und (EU-)-Gremien.

Der im jeweiligen Scope benannte TD

- führt grundsätzlich die Prüfungen des Genehmigungsobjekts und des CSMS/SUMS durch. Das KBA kann zusätzliche Prüfungen nach eigenem Ermessen durchführen.
- Leitet die relevante Information des Herstellers an das KBA weiter

[1] Im weiteren als Benennungsregeln bezeichnet
[2] Einzig verbindlich ist die deutsche Fassung. Übersetzungen dienen nur zur Information.

Der überprüfte Hersteller[3]

- gewährt den erforderlichen Zutritt und Zugriff auf Informationen
    - dem TD für die Dauer eines Überwachungszeitraums von 3 Jahren
    - dem KBA sowie dessen Beauftragten für die Dauer der Gültigkeit von Zertifikat und/oder Typgenehmigung
- stellt dem TD die im Rahmen der Bewertung erforderlichen Informationen, Dokumente und Aufzeichnungen (s. insbesondere Abschnitt B 2.3) zur Verfügung (eine gesonderte Übermittlung an das KBA ist entbehrlich, sofern dies nicht im Einzelfall ausdrücklich verlangt wird und unmittelbaren Einfluss auf die Gültigkeit von Zertifikat der Typgenehmigung haben könnte).

3 Erläuterungen zu Begriffen

Abweichung: unzureichende Erfüllung einer Anforderung

Anforderung: Erfordernis oder Erwartung, das oder die festgelegt, üblicherweise vorausgesetzt oder verpflichtend ist (EN ISO 9000; auch die dortigen Anmerkungen sind zu beachten)

Audit: Systematischer, unabhängiger und dokumentierter Prozess zur Erlangung von Nachweisen und deren objektiver Auswertung, um zu ermitteln inwieweit Auditkriterien erfüllt werden (vgl. EN ISO 9000). Im Anwendungsbereich der Benennung durch das KBA wird dieser Begriff gleichbedeutend mit Begutachtung Assessment u. Ä. verwendet.

Empfehlung: siehe Erklärung zu „sollte“

Funktionsprüfung: Prüfung, ob die vom Hersteller spezifizierten Sicherheitsmaßnahmen ihr Ziel erreichen (z. B. Prüfung eines gesicherten Kommunikationsprotokolls auf seine Eignung für ein Softwareupdate) (s. auch Anlage 2)

Prozessfähigkeit: Fähigkeit eines Prozesses, die von den Vorgabedokumenten und vom Hersteller definierten Ziele mit ausreichender Wahrscheinlichkeit zu erreichen

Re-Audit: Audit zum Zweck des Erlangens eines Folgezertifikats für denselben Scope, das unmittelbar an die Gültigkeit des vorigen Zertifikats anschließt. Das Audit ist im Regelfall während der Laufzeit des vorigen Zertifikats durchzuführen. Sofern zwischen Ablauf der Zertifikatsgültigkeit und Beginn des Audits mehr als 90 Tage vergangen sind, ist die Auditzeit wie für ein Erstaudit zu berechnen.

Sicherheitsprüfung: Aktiver Versuch des Prüfenden, Sicherheitsvorkehrungen zu umgehen (z. B. Penetration-Tests) (s. auch Anlage 2)

[3] im weiteren als Hersteller bezeichnet

Stufe-1-Audit: Audit mit folgenden Zielen:
- Bewertung der Bereitschaft zum Hauptaudit
- Bewertung der dokumentierten Information
- Ermittlung der standortspezifischen Bedingungen
- Sammeln von Informationen zum Geltungsbereich des CSMS/SUMS
- Präzisierung der Planung des Hautaudits, Ermittlung der notwendigen Ressourcen für das Hauptaudit

Details vgl. EN ISO/IEC 17021-1

Voraudit: Fakultative Bestandsaufnahme und Unterlagenprüfung vor Ort, durch die mögliche Schwachstellen in den Unterlagen und der Implementierung des Systems frühzeitig erkannt werden können. Es ist vergleichbar mit einer Generalprobe, aber in der Regel weniger umfangreich als das Hauptaudit.

Witnessing: Bewertung der Leistung von prüfenden/auditierenden Personen durch das KBA oder eine von diesem beauftragte Stelle. Der Bewertende nimmt in der Regel keinen direkten Einfluss auf die Tätigkeit des/der Prüfenden/Auditierenden.

In diesem Dokument bezeichnet:
- „muss“, „soll“, „es ist“ oder ähnliche Formulierungen: eine verbindliche Anforderung;
- „sollte“: eine anerkannte Möglichkeit zur Einhaltung der Anforderungen der UN-Regelung oder Benennungsregeln. Ein TD kann mindestens gleichwertige Optionen anwenden, vorausgesetzt, dies kann gegenüber dem KBA nachgewiesen werden.
- „kann“: eine Möglichkeit (Option zur Umsetzung)

Abkürzungen:

AFK	Anforderungskatalog
CS(MS)	Cybersecurity (Managementsystem)
ISMS	Informationssicherheitsmanagementsystem
KBA	Kraftfahrt-Bundesamt
MINT	Mathematik, Informatik, Naturwissenschaft, Technik
QM	Qualitätsmanagement
RASIC	Verantwortlicher, Entscheider, Unterstützender, zu Informierender, zu Beteiligender (Responsible, Accountable, Supportive, Informed, Consulted)
SU	Softwareupdate
TD	Technischer Dienst
TGV	Typgenehmigungsverfahren
UN-R	UNECE-Regelung
USB	Unterschriftsberechtigter

Teil A Benennung des Technischen Dienstes

A 1 Allgemeines

Die Benennung für die Prüfung im Scope CS/SU erfolgt auf Antrag in den Kategorien A, B und/oder D.

Sie erfolgt in einem neuen Prüfgebiet 14 und vergrößert somit die Stichprobe bei Überwachungsmaßnahmen.

14	Informationstechnologie/Künstliche Intelligenz/Cybersecurity“
14-01	Cybersecurity/Softwareupdate (Produktprüfung)
14-01-01	UN-R 155
14-01-02	UN-R 156
14-10	Prüfung von Managementsystemen im Prüfgebiet
14-10-01	UN-R 155
14-10-02	UN-R 156

Technische Dienste können nur dann für Prüfungen zu CS und/oder SU benannt werden, wenn sie gleichzeitig auch für die Prüfung von Gesamtfahrzeugen im Scope des jeweiligen CS/SU-Rechtsaktes benannt sind bzw. wenn sie enge Beziehungen zu einem für „Gesamtfahrzeug“ benannten TD nachweisen können (s. Nr. A 2).

Die Benennung für ein CSMS/SUMS kann nur erfolgen, wenn der Technische Dienst auch für damit in Verbindung stehende Produktprüfungen benannt ist. So ist z. B. die Benennung nach 14-01-01 Voraussetzung für eine Benennung nach 14-10-01.

A 2 Anforderungen an die Dokumentation des QM-Systems

Erforderliche QM-Dokumente bzw. Ergänzungen in vorhandenen QM-Dokumenten des TD:

- Verfahren zur Prüfung entsprechend UN-R 155/156
- Anforderungen an beteiligtes Personal
- Festlegungen zum Umgang mit vertraulicher Information (insbesondere mit CS/SU-relevanter Information
- bei Notwendigkeit: dokumentierte Interpretation von Forderungen der UN-R und des KBA

Entsprechende Informationen sind auf Verlangen in angemessenem Umfang auch dem Kunden zugänglich zu machen.

A 3 Anforderungen an das Personal

Es gelten die Anforderungen der Benennungsregeln mit folgender Ausprägung bzw. folgenden Zusätzen.

Grundsätzlich ist der Unterschriftsberechtigte (USB) sowohl für die Produkt- als auch für die Managementsystemprüfung in die Erfahrungskategorie 4 (s. Benennungsregeln) eingestuft. Die Berufserfahrung sollte nicht länger als 5 Jahre zurückliegen.

Das KBA kann auf Antrag Ausnahmen gewähren, behält sich in diesen Fällen aber ein intensives Witnessing vor.

A 3.1 Personal für Produktprüfungen

Anforderungen an eine(n) USB

- Akademischer Abschluss entsprechend Benennungsregeln (relevant sind insbesondere MINT-Studiengänge, die zumindest in Teilen Kenntnisse zum jeweiligen Einsatzgebiet vermitteln)
- ausgeprägte Kenntnisse zu Prüfungen entsprechend UN-R 155/156 im Sinne von Abschnitt B 3 (z. B. Penetration-, Fuzz-, Side-Channel-, Funktions-Tests)
- Kenntnisse zum Gesamtfahrzeug in Anlehnung an die relevanten Ausbildungsinhalte des KBA-Rahmenlehrplans für USB Gesamtfahrzeug (Ausbildung in einem TD mit Benennung zur Prüfung von Gesamtfahrzeugen)
- Kenntnisse und Fertigkeiten in der Anwendung von (Automotive-) Methoden zur Risikoanalyse
- Kenntnisse und Fertigkeiten zur Auditierung von Managementsystemen in der Automobilindustrie (möglichst auch CSMS/SUMS)

A 3.2 Personal für Prüfung des Managementsystems

Anforderungen an eine(n) USB

- Akademischer Abschluss entsprechend Benennungsregeln (relevant sind insbesondere MINT-Studiengänge, die zumindest in Teilen Kenntnisse zum jeweiligen Einsatzgebiet vermitteln)
- Expertenkompetenz gemäß ISO/IEC 27001 mit Schwerpunkt Cybersecurity in der Automobilindustrie, ISO 26262 mit Schwerpunkt Cybersecurity oder entsprechend mindestens gleichwertiger Anforderungen
- erfolgreich abgeschlossene Ausbildung als Auditor(in) von Managementsystemen (vergleichbar EOQ)
- mindestens 1 Jahr (3 Audits) Erfahrung als Auditor(in) in der Automobilindustrie
- Kenntnisse und Fertigkeiten in der Anwendung von (Automotive-) Methoden zur Risikoanalyse
- Kenntnisse zum Gesamtfahrzeug in Bezug auf das Zusammenwirken der Systeme und Komponenten.

Im Übrigen gelten die „Anforderungen an Mitarbeiter eines technischen Dienstes für die Auditierung eines CSMS gemäß der UN-R 155 und 156“ (s. Anlage 1).

Sofern die Anforderungen nach A 3.1 bzw. A 3.2 nicht erfüllt werden, wird Folgendes akzeptiert:

- der/die USB selbst hat Erfahrungen in der Auswahl, Durchführung/Beaufsichtigung und Bewertung der relevanten Prüfverfahren über mindestens ein Jahr (die Mitarbeit in entsprechenden Gremien wird angerechnet) und
- der/die USB hat Grundkenntnisse über das Zusammenwirken und das Risikopotenzial von Systemen und Bauteilen in einem Gesamtfahrzeug nachgewiesen. Der Nachweis wurde gegenüber dem Leiter eines TD „Gesamtfahrzeug“ oder einem/einer von diesem beauftragten USB und
- der/die USB wird für den noch fehlenden Teil von Kenntnissen/Fertigkeiten von entsprechenden Fachexperten unterstützt.
- Kenntnisse zum jeweiligen Einsatzgebiet können auch nach dem Studium erworben werden.

A 3.3 Aufrechterhaltung der Kompetenz

Die USB für Produktprüfungen und die USB für Prüfung des Managementsystems, alle in diesem Scope eingesetzten Auditoren/Auditorinnen sowie Fachexperten/Fachexpertinnen nehmen mindestens einmal pro Jahr an einem Erfahrungsaustausch zur Anwendung der UN-R 155/156 teil. Mindestens einmal in 3 Jahren sind dabei auch die Erfahrungen im eigenen TD auszutauschen. Der Erfahrungsaustausch kann im Zusammenhang mit dem sonstigen Erfahrungsaustausch des TD durchgeführt werden, muss sich aber für einen durch den Leiter des TD festzulegenden zeitlichen Anteil mit der Problematik der Auditierung/Typprüfung im Rahmen von CS/SU befassen.

Es ist anzustreben, dass sie bei vorhandenen Aufträgen mindestens einmal pro Jahr an entsprechenden Audits teilnehmen (die USB/Produkt und die Auditteamleiter/-leiterinnen auch an der Planung und Durchführung von Produktprüfungen sowie an der jährlichen Unterlagenprüfung).

Das KBA und der Leiter/die Leiterin des TD können weitergehende Festlegungen treffen.

Der Leiter/die Leiterin des TD dokumentiert die Anforderungen an das gesamte involvierte Personal in seinem/ihrem QM-System.

A 4 Verfahren der Benennung

A 4.1 Allgemeines

Das KBA kann für die Begutachtungen Fachexperten/-expertinnen hinzuziehen. Die Namen und auf Anfrage die Arbeitsstellen der Fachexperten werden dem TD mitgeteilt. Begutachter/ Begutachterinnen sowie Fachexperten/-innen dürfen bei ausreichender Begründung im Einzelfall vom TD abgelehnt werden.

A 4.2 Erstbenennung im Prüfgebiet

Die Entscheidung über die Benennung im jeweiligen Prüfumfang erfolgt im Ergebnis einer Geschäftsstellenbegutachtung und einer Witness-Begutachtung. Sie kann nach der Geschäftsstellenbegutachtung unter dem Vorbehalt einer erfolgreichen Witness-Begutachtung erfolgen. Über den Umfang von Maßnahmen bei Nachträgen im Prüfgebiet 14 entscheidet das KBA nach eigenem Ermessen.

Akkreditierungen für Prüfungen nach UN-R 155/156 bzw. ISO 21434 und ggf. sonstige Akkreditierungen werden angemessen berücksichtigt und können zur Verkürzung der Begutachtung führen.

A 4.3 Überwachung

Die Überwachung im Prüfgebiet 14 erfolgt entsprechend den allgemeinen Benennungsregeln.

Bei einer Benennung im Prüfumfang 14-10 erfolgt ergänzend mindestens 1 Witness-Begutachtung im Laufe eines Überwachungszeitraums (2,5 Jahre), sofern entsprechende Aufträge vorliegen. Der TD informiert das KBA zu diesem Zweck mindestens 4 Wochen vor jedem derartigen Audit.

Teil B Prüfungen durch den TD im Rahmen des TGV

B 1 Allgemeines

Ziel der Prüfungen ist es nachzuweisen, dass

- das installierte System angemessen, wirksam und effektiv ist, insbesondere die installierten Prozesse ausreichend fähig sind[4], die von den UN-R und dem Hersteller festgelegten Ziele und Funktionen umzusetzen,
- kein erhebliches Risiko für Sicherheit, Umwelt und Gesundheit im Rahmen des Scopes der UN-R 155/156 besteht,
- die vom Hersteller bereitgestellte Information verifiziert wurde,
- der Hersteller die von ihm dokumentierten Maßnahmen zufriedenstellend umgesetzt hat.

Es wird vom Hersteller erwartet, dass er Risiko- und sonstige Analysen sowie Maßnahmen/ Produkte nach den anerkannten Regeln der Technik entwickelt und umsetzt. Sofern er davon abweicht, hat er dies zu begründen. Der TD bewertet in diesem Fall die Angemessenheit und vermerkt dies im Bericht. Dies bezieht sich insbesondere auf kryptografische Methoden.

Sofern in Ermangelung der Vollkompetenz des/der USB Fachexperten/-expertinnen hinzugezogen worden sind, unterschreiben diese im internen Vorgang des TD für die Richtigkeit der jeweiligen Teilergebnisse, für die ihre Expertise genutzt wurde.

In diesem Fall darf die Bewertung desjenigen/derjenigen, der/die den Prüf-/Auditbericht unterschreibt grundsätzlich nicht besser sein, als die der jeweils erforderlichen Fachexperten. Ausnahmen von dieser Regel sind im Bericht oder im Anschreiben an das KBA mit Darstellung der abweichenden Meinungen zu begründen.

KBA und TD lagern Dokumente und Daten des Herstellers nur im absolut notwendigen Umfang und nur für die erforderliche Zeit in ausreichend geschützter Form. Aufbewahrungsfristen werden, sofern nicht in diesem Dokument anders geregelt, in den KBA-Empfehlungen für Aufbewahrungsfristen festgelegt. TD und KBA sind berechtigt, die Daten und Dokumente, die im Zusammenhang mit dem TGV gespeichert/gelagert werden, bei berechtigtem Interesse an Dritte herauszugeben, sofern der Hersteller nichts anderes festgelegt hat. Der TD informiert den Hersteller vor der beabsichtigten Herausgabe. Eine derartige Herausgabe wird dokumentiert.

[4] Ein mathematisch-statistischer Nachweis wird nicht gefordert.

B 2 Auditierung und sonstige Bewertung des CS- und SU-Managementsystems (CSMS/SUMS)

B 2.1 Allgemeines

Grundsätzlich erteilt das KBA Zertifikate für CSMS und SUMS gemäß UN-R 155/156 nur Herstellern von Gesamtfahrzeugen im Geltungsbereich der jeweiligen UN-R. Sofern andere Hersteller eine Auditierung zum Zweck der Erteilung eines solchen Zertifikats beantragen, wird dringend empfohlen, vor Annahme des Auftrags das KBA zu konsultieren.

Je Hersteller ist grundsätzlich immer das gesamte relevante Managementsystem zu auditieren und zu bewerten.

Sofern in diesem Dokument nichts anderes bestimmt ist, wird empfohlen, die grundsätzlichen Anforderungen der ISO/IEC 27006 in Anwendung auf die UN-R 155/156 anzuwenden.

Die TD übermitteln der KBA-Benennungsstelle neben den unter Nr. B 3 genannten Berichten Informationen über alle ihnen bekanntgewordenen und für die Typgenehmigung nach UN-R 155/156 relevanten Fakten.

B 2.2 Umfang und Art der Erstprüfung und Überwachung

Vor der erstmaligen Entscheidung über das Zertifikat und im Folgenden zumindest aller 3 Jahre (Re-Audit) (sofern der Genehmigungsinhaber am Fortbestand der Typgenehmigung interessiert ist) ist ein Vor-Ort-Audit (Hauptaudit) durchzuführen. Danach erfolgt im Abstand von jeweils 12 ± 1 Monaten zumindest eine Unterlagenprüfung.

Sofern der TD oder das KBA das aus gegebenem Anlass für erforderlich hält, können weitere Vor-Ort-Audits (z. B. Stufe 1-Audits, Nachaudits, anlassbezogene Audits) sowie Unterlagenprüfungen durchgeführt werden. Mehr als ein Voraudit je Erst- oder Erweiterungsantrag für das Zertifikat wird als Beratung angesehen und ist daher unzulässig.

Zwischen den Audits wertet der TD alle Informationen mit Bezug zum Zertifikat aus, die ihm zur Kenntnis gelangen. Der Hersteller wird vom Technischen Dienst verpflichtet, alle relevanten Informationen zur Verfügung zu stellen. Der TD leitet daraus ggf. erforderliche zusätzliche Überwachungsmaßnahmen ab und informiert das KBA im Fall einer wesentlichen Bedeutung für den Fortbestand des Zertifikats oder der Genehmigung.

B 2.3 Unterlagenprüfung

B 2.3.1 Allgemeines

Dokumente und Aufzeichnungen müssen geeignet sein, die Fähigkeit der relevanten Prozesse beim Hersteller sicherzustellen und nachzuweisen.

Hersteller, TD und KBA verständigen sich zu geeigneten Kommunikationswegen. Die Unterlagenprüfung kann ggf. auch vor Ort stattfinden. In diesem Fall ist die Unterlagenprüfung (außer Teile der Risikoanalyse) höchstens zu einem Drittel auf die Vor-Ort-Zeit entsprechend B 2.4 anzurechnen.

Die jährliche Unterlagenprüfung zwischen den Vor-Ort-Audits kann sich auf die mit (*) gekennzeichneten Unterlagen und auf sonstige Dokumente mit wesentlichen Änderungen beschränken.

Dokumentierte Informationen, Software und sonstige Auditnachweise, die sich im Besitz des Herstellers befinden, sind grundsätzlich bei diesen zu belassen, Kopien werden nicht angefertigt. Die Aufzeichnungen des Auditors/der Auditorin müssen aussagekräftig genug sein, um den Sachverhalt darzustellen und den objektiven Nachweis zu dokumentieren. Im Ausnahmefall können Originale oder Kopien von der Genehmigungsbehörde angefordert werden. Aus diesem Grund sind die Hersteller zu verpflichten, dass wesentliche Unterlagen für mindestens 12 Monate nach dem Audit aufbewahrt werden.

B 2.3.2 Mindestumfang der Unterlagenprüfung nach UN-R 155

Der zu Überprüfende legt dem TD zumindest folgende Dokumente und ggf. vorhandene Aufzeichnungen vor:

- Ausgefüllter Anforderungskatalog des KBA[5] und ggf. referenzierte Dokumente
- Geforderte Dokumente[6] nach UN-R 155 (vgl. Anhang 1 zur UN-R)
- Beschreibung des CSMS mit mindestens folgendem Inhalt
    - Allgemeine Grundsätze
    - Ggf. Ausschlüsse und Begründung dazu
    - Projektbezogenes Cybersecurity Management
    - * Kontinuierliche Cybersecurity Aktivitäten
    - Risikobewertungsmethoden
    - Cybersecurity Management im Produktlebenszyklus (Konzept, Entwicklung, Produktion, Betrieb und Wartung, Entsorgung)
    - Ggf. Sicherstellung der CS in Bezug auf Zulieferer/Dienstleister/ Unterauftragnehmer
    - CoP und Marktüberwachung in Bezug auf CS
    - Informationsmanagement in Bezug auf CS (intern, extern)
- Allgemeine Prozesslandschaft des Herstellers mit Darstellung der Cybersecurity-Aspekte
- Organigramme mit Darstellung der Cybersecurity-Aspekte
- Rollenbeschreibungen zu den CSMS-Prozessen (RASIC)
- Risikoanalyse mit zugehöriger Ausgangs- und Prüfinformation
- * Ggf. Liste der CSMS relevanten Zulieferer/Dienstleister/Unterauftragnehmer mit den jeweiligen Aufgaben und Verantwortlichkeiten und Bewertung des jeweiligen Risikos
- Prozessbeschreibungen, Prüfpläne und Prüfanweisungen sowie sonstige Dokumente mit Bezug zu CSMS

[5] Das KBA akzeptiert nach vorheriger Abstimmung auch mindestens gleichwertige Anforderungskataloge bzw. Berichte.
[6] Sollten die Inhalte der Dokumente eine Teilmenge der weiteren in diesem Abschnitt genannten Dokumente sein, so reicht eine einfache Dokumentation mit entsprechenden Hinweisen.

- * Ergebnisse durchgeführter Prüfungen/Audits (Übersicht)
- * CS-Vorfälle/Beinahe-Vorfälle und eingeleitete Aktivitäten (außer im Erst-Audit)
- * Aufzeichnungen zur Gewährleistung von CoP und zur Marktüberwachung in Bezug auf CS, insbesondere zu CS-Vorfällen (einschl. Angriffsversuchen)
- * Aufzeichnungen zu Anfragen Externer bzgl. CS

B 2.3.3 Mindestumfang der Unterlagenprüfung nach UN-R 156

Der zu Überprüfende legt dem TD zumindest folgende Dokumente und ggf. vorhandene Aufzeichnungen vor:

- Ausgefüllter Anforderungskatalog des KBA[5] und ggf. referenzierte Dokumente
- Geforderte Dokumente nach UN-R 156 (vgl. Anhang 1 zur UN-R)
- Beschreibung des SUMS mit mindestens folgendem Inhalt
    - Allgemeine Grundsätze
    - Ggf. Ausschlüsse und Begründung dazu
    - Risikobewertungsmethoden (u. a. auch Sicherheitsrisikoanalyse)
    - SU Management im Produktlebenszyklus (Konzept, Entwicklung, Produktion, Betrieb und Wartung, Entsorgung)
    - Identifikations- und Berichtsmöglichkeiten in Bezug auf die jeweils im Fahrzeug installierte und freigeschaltete Software
    - Ggf. Liste der SUMS relevanten Zulieferer/Dienstleister/Unterauftragnehmer mit den jeweiligen Aufgaben und Verantwortlichkeiten mit Bewertung des jeweiligen Risikos
    - CoP und Marktüberwachung in Bezug auf SU
    - Informationsmanagement in Bezug auf SU (intern, exten)
- Allgemeine Prozesslandschaft des Herstellers mit Darstellung der SUMS-Aspekte
- Organigramme mit Darstellung der SU-Aspekte
- Rollenbeschreibungen zu den SUMS-Prozessen (RASIC)
- Risikoanalyse zum SUMS mit zugehöriger Ausgangs- und Prüfinformation
- * Ggf. Liste der SU-relevanten Zulieferer/Dienstleister/Unterauftragnehmer/sonstiger relevanter Parteien mit den jeweiligen Aufgaben und Verantwortlichkeiten und Bewertung des jeweiligen Risikos
- Prozessbeschreibungen, Prüfpläne und Prüfanweisungen sowie sonstige Dokumente mit Bezug zum SUMS
- * Ergebnisse durchgeführter Prüfungen/Audits (Übersicht)
- * Aufzeichnungen zur Gewährleistung von CoP und zur Marktüberwachung in Bezug auf SU, insbesondere zu SU-Vorfällen (einschl. Angriffsversuchen)
- * Aufzeichnungen zu Anfragen Externer bzgl. SU

B 2.4 Vorgaben für das Vor-Ort-Audit

Es gelten, soweit anwendbar, die Festlegungen der ISO/IEC 27006. Ein formelles Stufe 1-Audit kann durchgeführt werden, ist aber nicht gefordert. In jedem Fall sind die Inhalte der Stufe 1 zu bearbeiten.

Dem Vor-Ort-Audit geht eine Unterlagenprüfung voraus.

Das KBA empfiehlt, bei der Berechnung der Auditzeit die Methodik nach ISO/IEC 27006 und folgende Randbedingungen zu beachten:

- Ausgangswert sind die Tabellenwerte der EN ISO/IEC 27006, angewendet auf zumindest alle im jeweils zu prüfenden Scope relevanten Mitarbeiter und sonstigen Führungskräfte (z. B. aus der Entwicklung, Produktprüfung, Auditoren usw.) sowie die Leitung der Fachbereiche an den Standorten einschließlich Zentrale (z. B. Qualitätsplanung, Produktion, Beschaffung usw.). Es wird empfohlen, von ca. 7 % der Gesamtmitarbeiterzahl im Scope des Zertifikats auszugehen. Die Kalkulation erfolgt im Einverständnis mit dem Auditleiter/der Auditleiterin (Unterschreibende) auf Basis der Festlegungen im TD. In Anbetracht dessen, dass ein CSMS/SUMS nur Teile eines ISMS umfasst, kann von einem „normalen“ Aufwand“ und „mittlerer Komplexität“ nach EN ISO/IEC 27006 ausgegangen werden.
- Die so bestimmte Zeit ist entsprechend Ergebnissen der Unterlagenprüfung, Erfahrungen aus früheren Audits, Komplexität der Produkte und/oder Prozesse, Risikobewertung, Zeiten für Übersetzungen u. Ä. zu erhöhen. Sie kann aus gleichem Grund um max. 20 % reduziert werden (z. B. keine Entwicklungsverantwortung, einfache Produkte/Prozesse, Erfahrungen aus früheren Audits).
- Für Re-Audits ist von 2/3 des berechneten Werts auszugehen (s. auch „Erläuterungen zu Begriffen“).
- Mindestens 70 % der so errechneten Zeit, aber nicht weniger als 32 Stunden (Re-Audit: 24 Stunden) sind vor Ort zu auditieren. Bei begründeten Abweichungen ist vorab die Zustimmung des KBA einzuholen. In dieser Vorgabe ist täglich bis zu 1 Stunde Auditorenzeit und Tageszusammenfassung/sonstige Abstimmung (am Abschlusstag: 2 Stunden) sowie maximal 1 Stunde/Tag Wegezeit berücksichtigt. Pausen und sonstige (z. B. Reise-) Zeiten sind zusätzlich zu planen.

Die stichprobenartige Auditierung von Produktprüfungen durch den Hersteller ist Bestandteil des Audits (als Nachweis der Prüfkompetenz) Diese Zeit kann nach Ermessen des TD auch im Rahmen der Typprüfung berücksichtigt werden). Es wird vorgeschlagen, dafür 4 Stunden zu planen.

Bei mehreren Standorten sollte die Methodik nach IAF MD1 angewendet werden.

Eine Trennung des Auditteams für einzelne Phasen ist nur zulässig, wenn in jeder Auditphase der Auditor/die Auditorin bzw. das (Teil-)Auditteam über ausreichende Kompetenz zur Bewertung von CS/SU sowie von Managementsystemen verfügen (s. A 3 „Anforderungen an das Personal“).

Anhand der Prüfung von Dokumenten und Aufzeichnungen, von Interviews und Beobachtung realer Prozessabläufe und Prüfungen sind alle relevanten Anforderungen entsprechend KBA-Anforderungskatalog[5] zu bewerten. Bei Re-Audits sind die Ergebnisse von Überprüfungen in den zurückliegenden 3 Jahren zu berücksichtigen.

Doppelprüfungen sind zu vermeiden. Über den Umfang der Anerkennung sonstiger Prüfzeugnisse (z. B. Zertifizierungen nach ISO 21434 oder UN-R-155/156) und damit die Reduzierung der Auditzeit entscheidet der TD. Eine vorherige Abstimmung mit dem KBA wird empfohlen. Entscheidung und Begründung dafür sind im Audit- bzw. Prüfbericht zu dokumentieren.

Die Auditierung der Post-Production-Phase/Nach-Nutzungsphase/Marktüberwachung bezieht sich nur auf die vom Hersteller zu beeinflussenden Faktoren und wird sich schwerpunktmäßig auf den entsprechenden Teil der Risikoanalyse und die daraus resultierenden Maßnahmen (auch an externen Standorten, wie z. B. herstellereigenen oder sonstigen von Hersteller betreuten Servicestützpunkten) konzentrieren.

Zulieferer, Dienstleister u. Ä. werden grundsätzlich nur in Bezug auf die Absicherung der Nahtstelle durch den Hersteller in das Audit einbezogen.

B 2.5 Einstufung von Feststellungen

Die Einstufung der Ergebnisse erfolgt gemäß den Forderungen der ISO/IEC 27006.

Feststellungen können im Ergebnis der Unterlagenprüfung und des Vor-Ort-Audits getroffen werden. Bei der Bewertung sonstiger Informationen ist in Anlehnung an die Klassifizierung zu verfahren.

Es wird unterschieden in

- Positive Feststellungen
- Verbesserungspotenzial
- Nebenabweichung
- Hauptabweichung.

Positive Feststellung: Erfüllung der Anforderungen über das zu erwartende Maß hinaus.

Verbesserungspotenzial: Möglichkeiten zur Verbesserung bei grundsätzlicher Erfüllung der Anforderung

Nebenabweichung:
- Unzulänglichkeit bei der Erfüllung einer Anforderung, die die Fähigkeit des Management-systems, die beabsichtigten Ergebnisse zu erreichen, nicht beeinträchtigt.
- Verbesserungspotenzial, das nicht bewertet worden ist, führt zu einer Nebenabweichung in Bezug auf den Verbesserungsprozess.

Nebenabweichungen führen zu einem Aussetzungsverfahren, wenn sie nicht fristgerecht abgeschlossen werden. Wenn durch die Anzahl der Nebenabweichungen auf ein Versagen des Qualitätsmanagementsystems geschlossen werden muss, führt das zu den Folgen wie bei einer Hauptabweichung.

Hauptabweichung:
Nichterfüllung einer Anforderung, die die Fähigkeit des Managementsystems, die beabsichtigten Ergebnisse zu erreichen, beeinträchtigt. Dies ist unter anderem in folgenden Fällen anzunehmen:

- erheblicher Zweifel, dass eine wirksame Prozesslenkung besteht oder dass Produkte bzw. Dienstleistungen die festgelegten Anforderungen erfüllen
- erhebliche Zweifel an der Qualität von Risikoanalyse, der im Ergebnis eingeleiteten Maßnahmen, an der Prüfplanung, an Prüfungen und an Entscheidungen zur Erfüllung der Anforderungen (u. a. in Bezug auf Erreichen eines akzeptablen Risikos)
- Produktprüfungen führen wiederholt zu negativen Ergebnissen, die ähnliche Ursachen haben
- Der Genehmigungsinhaber weicht von den Bestimmungen der UN-R, sonstiger relevanter Rechtsakte und/oder der Genehmigung ab und ergreift nicht unverzüglich adäquate Korrekturen und Korrekturmaßnahmen.
- eine Abweichung bzgl. der Wirksamkeit von Korrekturmaßnahmen aus den zurückliegenden 5 Jahren, die wiederholt festgestellt wurde
- sonstige schwerwiegende Verstöße gegen genehmigungsrelevante Anforderungen.

Hauptabweichungen sind umgehend durch ein Vor-Ort-Nachaudit zu schließen. Das Vor-Ort-Audit wird für einen Termin spätestens 90 Tage nach Abschluss des Hauptaudits geplant. Hauptabweichungen hemmen die Ausstellung des Zertifikats. Sofern sie während der Laufzeit des Zertifikats festgestellt werden, führen bei nicht fristgerechter Erledigung zur Aussetzung des Zertifikats (nach Ermessen des KBA auch eines Teils des Zertifikats).

Für Nebenabweichungen müssen zumindest Maßnahmepläne vom TD akzeptiert worden sein, um diese zu schließen. Die Wirksamkeit der Maßnahmen ist beim nächsten Audit zu prüfen.

Über die Einstufung entscheidet der/die Auditteamleiter/-leiterin, also derjenige/diejenige, der/die den Auditbericht unterschreibt. Bei Einsatz von Fachexperten ist Nr. B 1 zu beachten.

B 2.6 Beim KBA einzureichende Unterlagen

Im Ergebnis des Vor-Ort-Audits und der jährlichen Unterlagenprüfung zwischen den regulären Audits übergibt der TD der KBA-Benennungsstelle:

- Bericht entsprechend ISO/IEC 27006 in Bezug auf die Erfüllung der Anforderungen entsprechend UN-R 155/156. Im Bericht sind Besonderheiten des Audits bzw. der Unterlagenprüfung, wie z. B. die Berücksichtigung anderer Zertifikate, Ausschluss von Anforderungen usw., mit Begründung darzustellen. Der ausgefüllte KBA-Anforderungskatalog[7] und die zugehörigen Checklisten sowie die Feststellungsprotokolle sind dem Bericht als Anlage beizufügen.[5]
- Den vom Hersteller jährlich zu erstellenden Bericht über dessen Überwachungsaktivitäten (nur UN-R 155) und eine Bewertung aller derartiger Berichte und sonstigen Informationen des Herstellers im Überwachungszeitraum (nur bei der jährlichen Unterlagenprüfung)

[7] kann bei der Unterlagenprüfung entfallen

- Nachweis über eine Qualitätsprüfung des Berichts entsprechend den Festlegungen des TD (mindestens durch einen CS- und MS-Experten, der nach Möglichkeit nicht am Audit teilgenommen hat)
- Liste der eingesehenen Dokumente[8]
- Liste der objektiven Nachweise.[8]

Der Bericht ist umgehend einzureichen, wenn er eine positive Empfehlung zur Zertifikatserteilung enthält und alle Hauptabweichungen geschlossen sind (Nebenabweichungen können noch offen sein bzw. müssen noch nicht abschließend auf die Wirksamkeit der eingeleiteten Maßnahmen bewertet sein.

Das KBA ist immer dann umgehend zu informieren, wenn Sachverhalte bekannt werden, die Auswirkungen auf die Gültigkeit des Zertifikats oder der Genehmigung haben könnten. Dies ersetzt nicht die Pflicht des Herstellers, das KBA in solchen Fällen umgehend direkt zu informieren.

B 3 Produktprüfung

B 3.1 Allgemeine Anforderungen

- Die Prüfung schließt neben der praktischen Prüfung am Produkt auch die Prüfung der zugehörigen Dokumentation ein (z. B. Vollständigkeit der Risikoanalyse und Angemessenheit der abgeleiteten Schlussfolgerungen). Im praktischen Teil wird u. a. bewertet, ob mit den vom Hersteller geplanten Maßnahmen das beabsichtigte Mindestsicherheitsziel und der geforderte Funktionsumfang erreicht werden kann.
- Mindestens 1 Prüfung je UN-R ist vom TD praktisch durchzuführen/zu beaufsichtigen. Umfang und Inhalt der Prüfungen sollten, ausgehend
  - von der Risikoanalyse und dem daraus abgeleiteten worst-case und
  - dem definierten Sicherheitsziel des Herstellers (ggf. auch in der post-production-phase) und
  - dem geforderten Mindestsicherheitsziel und dem ggf. in den UN-R geforderten Funktionsumfang und
  - den Empfehlungen in Anlage 2

  geplant werden. Weitere Prüfung werden durch den TD in Abhängigkeit von Prüfergebnis, Kompetenz des Durchführenden (bei Beaufsichtigung) usw. durchgeführt/beaufsichtigt. Die Prüfungen sollen sich auf wesentliche Risiken konzentrieren. Der worst-case kann die Prüfung an mehreren Fahrzeugen erfordern.
- Das zu erwartende Mindestsicherheitsziel ergibt sich aus den jeweiligen UN-R und muss, insbesondere in der Übergangsphase der Einführung der UN-R 155, zur Erfüllung der allgemeinen Forderung nach Vermeidung erheblicher Risiken für Sicherheit, Umwelt und Gesundheit beitragen. Präzisierungen werden im Rahmen des Erfahrungsaustauschs zu einem späteren Zeitpunkt getroffen.
- Neben dem Fahrzeug sollte zumindest auch das Back-end bei der Auswahl der Prüfungen berücksichtigt werden.

[8] sofern nicht bereits aus dem ausgefüllten Anforderungskatalog erkenntlich

- Wesentliche Behauptungen des Herstellers, wie z. B. die, dass eine Komponente nicht updatefähig ist oder ein Update keine weiteren Teile/Systeme des Fahrzeugs beeinflusst, sind zu überprüfen.
- Sofern der TD über die erforderliche Prüfausrüstung verfügt, sollte die Prüfung in der eigenen Laborumgebung des TD stattfinden. Ggf. sollte der Hersteller bei der Durchführung unterstützen (z. B. durch Bereitstellung von Analysetools).
- Die Beaufsichtigung kann sich auf wesentliche Phasen beschränken (z. B. Risikoanalyse, verwendete Hard- und Software, Versuchsaufbau, Teilergebnisse, Prüfung von Aufzeichnungen). Die Beaufsichtigung beim Hersteller sollte nach Möglichkeit auch zur Bewertung der Prüfkompetenz im Rahmen der CSMS/SUMS-Auditierung dienen (u. a. geeignete Ressourcen, kompetente Durchführung). Der beaufsichtigende TD definiert die Vorgaben zur Art der Prüfung, Nutzung bestimmter Geräte, zur Schaffung bestimmter Prüfumgebungen, zu Angriffspfad- und -ziel, zum Fahrzeug usw.
- Bei Beaufsichtigung von Prüfungen bzw. Nutzung fremder Prüfausrüstung ist die Integrität der genutzten Hard- und Software nachvollziehbar sicherzustellen. Die Nachvollziehbarkeit der Prüfungen ist über einen Zeitraum von mindestens 10 Jahren nach endgültiger Einstellung der Produktion zu gewährleisten (u. a. „Versiegelung“ der Software).

Hinweise zur Durchführung von Produktprüfungen sind diesem Dokument als Anlage 2 beigefügt.

Sofern Fachexperten hinzugezogen werden, ist Nr. B 1 zu beachten.

B 3.2 Beim KBA einzureichende Unterlagen

Die Dokumentation (der Prüfbericht) muss neben den Anforderungen aus den Benennungsregeln, insbesondere aus Anhang 5, mindestens beinhalten:

- Prüfplan und die Begründung dafür (analog der Anforderungen an den Prüfplan des Herstellers, s. Anlage 2 Nr. 2.2
- die erwarteten Prüfergebnisse (insbesondere, sofern in der UN-R keine speziellen Vorgaben enthalten sind)
- die tatsächlichen Prüfergebnisse
- Begründung für akzeptierte Abweichungen (einschließlich „Lücken“ in der Risikoanalyse u. Ä.)
- Besonderheiten, wie z. B. Nutzung von Hard- und Software zu Prüfzwecken, die nicht Eigentum des TD ist und Maßnahmen zur Sicherstellung der Integrität

Die Schlussbescheinigung muss sich auf den Aussagen zu vorstehend genannten Inhalten gründen.

Anlage 1

Anforderungen an Mitarbeiter eines technischen Dienstes für die Auditierung eines CSMS gemäß der UN-R 155 und 156

Die ISO 17021-1 liefert allgemeine Grundlagen für Aktivitäten im Bereich der Zertifizierung von Managementsystemen und ist aufgrund der Anforderungen an technische Dienste zu berücksichtigen. Zur Umsetzung der UN-R 155 und 156durch technische Dienste ist zur Festlegung der Auditorenanforderungen die Einbeziehung der ISO/IEC 27006, angewendet auf die automotive Cybersecurity naheliegend.

In diesem Anhang werden die Anforderungen der Normen ISO/IEC 17021-1 und ISO/ IEC 27006 als Basis für die Rollen innerhalb eines technischen Dienstes dargestellt. Eine detaillierte Aufstellung der Anforderungen lässt sich in den folgenden Tabellen finden, in denen die notwendigen Rollen und deren Kompetenzen und das notwendige Wissen eines Auditteams beschrieben sind

Die verwendeten Kürzel für die Zertifizierungsfunktionen haben die folgende Bedeutung:

AP	(Antragsprüfer):	Durchführung der Antragsprüfung, um im Einverständnis mit dem Leitenden Auditor die erforderlichen Kompetenzen des Auditteams zu ermitteln, die Mitglieder auszuwählen und den Auditzeitaufwand festzulegen
BP	(Berichtsprüfer):	Überprüfung der Auditberichte und Vorschlag für die Zertifizierungsentscheidung
LA	(Leitender Auditor)	Planung des Audits Auditierung und Leitung des Auditteams; Unterschrift unter dem Auditbericht

1 Allgemeine Anforderungen

Funktion	Wissen und Fertigkeiten		Normenverweis für LA
	ISO/IEC 17021-1	ISO/IEC 27006	
BP, LA		Wissen über Information Security Management Terminologie, Prinzipien, Praktiken und Techniken	ISO/IEC 27006 7.1.2.1.2
LA	Wissen über praktische Unternehmensführung	Wissen über praktische Unternehmensführung	ISO/IEC 27006 7.1.2.1.4 ISO/IEC 17021-1 A.2.1
BP, LA	Wissen über Auditgrundsätze, -praktiken und -techniken		ISO/IEC 17021-1 A.2.2
AP, BP, LA	Wissen über spezifische Management Systemnormen und normative Dokumente	Wissen über Informations-/Security Management Systemnormen und normative Dokumente	ISO/IEC 27006 7.1.2.1.3 ISO/IEC 17021-1 A.2.3
AP, BP, LA	Wissen über Prozesse der Zertifizierungsstelle		ISO/IEC 17021-1 A.2.4
AP, LA, (BP durch ISO 27006)	Wissen über Produkte, Prozesse und Organisation des Kunden	Wissen über Produkte, Prozesse und Organisation des Kunden	ISO/IEC 27006 7.1.2. ISO/IEC 17021-1 A.2.6
LA	Sprachliche Fertigkeiten, um auf allen Ebenen innerhalb der Organisation des Kunden angemessen zu kommunizieren		ISO/IEC 17021-1 A.2.7
LA	Fertigkeiten für die Aufzeichnung von Notizen und die Erstellung von Berichten		ISO/IEC 17021-1 A.2.8
LA	Präsentationsfertigkeiten		ISO/IEC 17021-1 A.2.9
LA	Fertigkeiten für das Durchführen von Befragungen		ISO/IEC 17021-1 A.2.10
LA	Fertigkeiten zum Managen von Audits		ISO/IEC 17021-1 A.2.11

2 Spezialwissen im Auditteam

Da die beschriebenen Anforderungen weitestgehend generisch gehalten sind, gilt es, diese Anforderungen weiter zu spezifizieren. In Anlehnung an die ISO 27006, 27002 und ISO 21434 soll ein Auditor bzw. ein Auditoren-Team über das Wissen in den folgenden Bereichen verfügen:

Themenbereich	Thema	Basis
CSMS allgemein	Organisation Governance Compliance Datenschutz (Privacy), Geistiges Eigentum, ISMS	UN-R 155 ISO 27001 ISO 27002 ISO 21434 DSGVO
Cyber Security Management	Asset Management Security Ziele Management von Vorfällen Schwachstellen-Management Projektbezogenes Cybersecurity Management Arbeit mit externen Dienstleistern fortlaufende Cybersecurity-Aktivitäten	UN-R 155 ISO 21434
Produktlebenszyklus	Konzeptphase Entwicklungsphase Produktionsphase Nach-Produktionsphase	UN-R 155 ISO 21434
Bedrohungs- und Risikoanalyse	Asset Identifikation Bedrohungsindentifikation Analyse von Einflussfaktoren Analyse von Angriffspfaden Wahrscheinlichkeitsanlyse Bewertung, Behandlung	UN-R 155 ISO 21434
Bedrohungen	Back-End Server Interne Fahrzeugkommunikation Externe Fahrzeugkommunikation Updateverfahren Menschliches Fehlverhalten Codeschwachstellen Physische Manipulation	UN-R 155
CybersecurityTest	Penetration Test Fuzz testing Statische Codeanalyse Schnittstellentests Vulnearability scanning Simulation Hardware	UN-R 155 ISO 21434

Themenbereich	Thema	Basis
Cybersecurity	Schwachstellen in der Kryptographie Kommunikationsicherheit Integrität Vertraulichkeit Wechselwirkung	UN-R 155 ISO 21434

Die Forderungen der UN-R 156 sind sinngemäß anzuwenden.

Anlage 2

Hinweise zu Produkttests und Schwachstellenanalysen gemäß UN-R 155 und UN-R 156 Leitfaden[9]

Anlage zum KBA-Dokument
„Anwendung der Benennungsregeln für Technische Dienste zu Prüfungen nach UN-R 155/156“
(Teil B Abschnitt 3)

1 Vorbemerkungen und Definitionen

1.1 Funktions- und Sicherheitstests

Dieses Dokument behandelt zwei Arten von Tests, die der Übersichtlichkeit halber getrennt behandelt werden. Zum einen handelt es sich um Tests zur Prüfung der Funktionen (Funktionstests) und Tests zur Prüfung der Cybersicherheit (Sicherheitstests). Funktionstests bestätigen die Erfüllung der (funktionalen) Anforderungen und Sicherheitstests - die Erfüllung der IT-Sicherheitsziele.

Sicherheitstests sind jene Untersuchungen, bei denen reale und aktuelle Angriffe nachgeahmt werden, um Möglichkeiten zur Gefährdung der Cybersicherheitsziele zu ermitteln. Es gilt zu prüfen ob ein Angreifer unter Ausnutzung von (ggf. unbekannten) Schwachstellen des betrachteten Systems (hier: von Fahrzeug bis Backend-Infrastruktur) unautorisiert auf Daten oder Ressourcen des Systems zugreifen kann.

In Abgrenzung zur funktionalen Sicherheit wird bei Sicherheitstests im Sinne der UN-R 155/156 nicht gegen natürliche, heuristische Fehler (wie z. B.: Softwarefehler, (E/E-) Komponenten-versagen, Konfigurationsfehler, etc.) geprüft/entwickelt, sondern gegen absichtliche Angriffe, welche ggf. komplexe Angriffsvektoren und erzwungene Systemzustände beinhalten.

Implementierte Sicherheitsmaßnahmen wie z. B. kryptographische Protokolle können aber ebenfalls reinen Funktionstests (keine Sicherheitstests im Sinne dieser Definition) unterzogen werden. Es wird zunächst getestet, ob sich der Sicherheitsmechanismus gemäß Spezifikation verhält, ohne zu versuchen, diesen aktiv zu umgehen.

[9] Der Leitfaden einschließlich der Empfehlungen wurde vom Bundesamt für Sicherheit in der Informationstechnik in Zusammenarbeit mit dem KBA entwickelt und vom KBA als Anhang zu diesem Dokument freigegeben.

1.2 Zusammenhang UN-R 155 und 156 (Cybersecurity)

Vorangestellt sei, dass beide UN-Regelungen selbstverständlich unabhängig voneinander sind und dementsprechend Produkte nach der einen oder anderen Regel genehmigt werden können.

Die Absicherung der Cybersicherheit ist die genuine Aufgabe der UN-R155. Zusätzlich enthält die UN-R 156 Cybersicherheit-Anforderungen (z. B.: 7.1.3. Security […]), welche entweder im Rahmen der Prüfung nach UN-R 155 mit berücksichtigt werden können[10] oder in einem gesonderten Sicherheitstest für die Typgenehmigung nach UN-R 156 berücksichtigt werden müssen. Sofern die Überprüfung/Typgenehmigung für beide Regelungen in zeitlichem Zusammenhang erfolgt, wird dem TD und der Genehmigungsbehörde[11] empfohlen, die Prüfpläne für beide Regelwerke unter diesem Gesichtspunkt zu kombinieren.

1.3 Weitere Dokumente

Die Produktentwicklung nach dem Stand der Technik erzeugt eine Vielzahl hilfreicher Dokumente (z. B.: zukünftig work products nach ISO/SAE 21434 usw.), welche im Rahmen der Typgenehmigung genutzt werden sollten, um zielgerichtet und effizient prüfen zu können.

Zusätzlich geforderte Dokumente werden in den Besonderen Festlegungen des KBA spezifiziert

2 Prüfaspekte in Beguzug auf die Cybersicherheit

2.1 Prüfung der Herstellerdokumentation

Die Risikoanalyse und die Dokumentation der Herstellertests bilden die Grundlage für die Prüfungen des technischen Dienstes.

Die Dokumentation sollte einen Testplan (und die Begründung dafür), die erwarteten Testergebnisse und die tatsächlichen Testergebnisse enthalten.

Der Testplan sollte für jede betrachtete Schnittstelle/Komponente des Fahrzeugs eine Beschreibung der durchgeführten Testszenarien und Tests beinhalten. Er sollte auch auf ggf. vorhandene Abhängigkeiten (z. B. Test B erfordert die Ergebnisse von Test A) eingehen.

Der TD bewertet die Vollständigkeit des Testplans und die Übereinstimmung der erwarteten mit den tatsächlichen Ergebnissen der Herstellertests, siehe auch Abschnitt 3.

[10] ggf. als Erweiterung des Umfangs der Bedrohung/Verletzbarkeit von Updateprozessen (vgl. Tabelle A1, Anhang 5, UN-R 155)
[11] Im Folgenden umfasst der Begriff TD immer auch die Genehmigungsbehörde, sofern dies nicht ausdrücklich anders dargestellt wird.

2.2 Praktische Tests durch den TD

Folgende Aspekte sind vor einer Testdurchführung des technischen Dienstes zu klären:

2.2.1 Eigene Tests

Werden nur Tests der Hersteller nachvollzogen oder zusätzlich selbst konzipierte (Funktions- oder Sicherheits-) Tests durchgeführt/beaufsichtigt?

Empfehlung

Es sollten durch den TD selbst konzipierte Funktions- und Sicherheitstests durchgeführt werden, insbesondere dann, wenn Lücken im Testplan erkennbar sind.

2.2.2 Testumfang bzw. -abdeckung

Für wie viele und welche Schnittstellen des Fahrzeugs werden Tests durch den TD nachvollzogen bzw. durchgeführt/beaufsichtigt?

Empfehlung

Unter Berücksichtigung der zur Verfügung stehenden (insbesondere zeitlichen) Ressourcen sollte (als vorläufige Vorgehensweise) eine Menge von Schnittstellen des Fahrzeugs individuell durch den TD ausgewählt und getestet werden. Bei der Auswahl sollte die Risikoanalyse berücksichtigt werden. Mittelfristig sollten die (mindestens) zu prüfenden Schnittstellen/Komponenten in einem Best-Practice-Leitfaden definiert werden.

Werden nur externe Schnittstellen des Fahrzeugs getestet oder auch (nicht direkt von außen zugängliche) interne Komponenten und Schnittstellen?

Empfehlung

Bei der oben erwähnten Auswahl sollten vorrangig externe Schnittstellen berücksichtigt werden, da für diese ein erhöhtes Risiko zu erwarten ist. In bestimmten Fällen (falls die Sicherheit besonders von einer internen Komponente abhängt) können auch interne Komponenten stichprobenartig getestet werden.

Siehe auch Abschnitt 3.

2.2.3 Testumgebung

In welcher Umgebung werden die Tests durchgeführt?

Optionen

- In den Räumlichkeiten des Herstellers. TD beaufsichtigt die Testdurchführung.
- In den Räumlichkeiten des TDs. Hersteller stellt geeignetes Testobjekt und Testequipment zur Verfügung.
- In den Räumlichkeiten des TDs. Hersteller stellt geeignetes Testobjekt zur Verfügung. TDs nutzt ausschließlich eigenes oder selbst angemietetes Testequipment.

Empfehlung

Sofern der TD über die erforderliche Prüfausrüstung verfügt, sollte der Test in der eigenen Laborumgebung des TD stattfinden.

Die Verantwortung für die Eignung […] der bei der Prüfung verwendeten Geräte und Methoden liegt einzig beim TD, egal ob dieser der Eigentümer derselben ist oder nicht (vgl. ISO/IEC 17020:2012).

Einschlägige Normen zur Schaffung von Vertrauen in die Arbeiten von Laboratorien/ Inspektionsstellen und Anforderungen an diese (z. B.: ISO/IEC 17020, ISO/IEC 17025) sollten sinngemäß auf die besonderen Herausforderungen der Cybersicherheit interpretiert und angewandt werden. Begründet wird dies mit der aktiven Natur der „Fehlerquelle“, die hier vorsätzlich, schlimmstenfalls während der Prüfung der Systeme, auftreten kann.

Bei Beaufsichtigung von Tests bzw. Nutzung fremder Prüfausrüstung ist die Integrität, die korrekte Konfiguration und ggf. korrekte Kalibrierung der genutzten Prüf-Hard- und -Software daher nachvollziehbar sicherzustellen. Die Nachvollziehbarkeit des Tests ist über einen Zeitraum von mindestens 10 Jahren nach endgültiger Einstellung der Produktion zu gewährleisten (u. a. Dokumentation und ggf. „Versiegelung“ der eingesetzten Prüf-Hard- und -Software).

2.2.4 Angriffsniveau (für Sicherheitstests)

Welches Angriffsniveau wird angenommen?

Das Angriffsniveau wird z. B. durch folgende Faktoren bestimmt:

- Zur Verfügung stehende Zeit
- Expertise des Angreifers
- Vorliegende Kenntnisse über den Untersuchungsgegenstand (White-Box-, Grey-Box-, Black-Box-Testing)
- Zur Verfügung stehende Werkzeuge (im Handel erhältliche Tools, Spezialwerkzeuge, Herstellertools, selbst entwickelte Tools…)

Optionen

- Es wird ein allgemeines Mindestniveau festgelegt.
- Das Angriffsniveau wird im Einzelfall abhängig von der durch den Hersteller durchgeführten Risikoanalyse oder einer eigenen Risikobetrachtung des TDs festgelegt.

Empfehlung

Grundsätzlich sollte das Angriffsniveau umso höher gewählt werden, je größer das Risiko durch eine betrachtete Komponente/Schnittstelle eingeschätzt wird. In der Regel sollten White- oder Grey-Box-Tests durchgeführt werden, da die entsprechende Dokumentation des Herstellers vorliegen sollte.

2.2.5 Vorbereitende Analysen (für Sicherheitstests)

Welche vorbereitenden Analysen werden durchgeführt?

Optionen

- Es werden nur Sicherheitstest nachvollzogen, die der Hersteller bereits selbst durchgeführt hat.
- Es wird eine Menge von vorab definierten „Standardtests“ (Brute-Force-Angriffe, Fuzzing o. Ä.) durchgeführt.
- Es wird nach Schwachstellen im Untersuchungsgegenstand mit Hilfe öffentlich zugänglicher Informationsquellen/Datenbanken oder ggf. eigener Datenbanken des TD recherchiert. Bei positivem Ergebnis werden die entsprechenden Angriffe durchgeführt, sofern sie das festgelegte Angriffsniveau nicht überschreiten.
- Auf Grundlage der vorliegenden Designunterlagen und funktionalen Spezifikationen werden potenziell angreifbare Schnittstellen identifiziert. Es werden individuell spezifizierte Angriffsversuche (auf gegebenem Angriffsniveau) durch einen erfahrenen Pentester auf diese Schnittstellen durchgeführt.

Empfehlung

Es sollte eine unabhängige Recherche nach bekannten Schwachstellen durchgeführt werden. Individuell spezifizierte Pentests durch den TD werden nachdrücklich empfohlen.

2.3 Anforderungen der UN-R 156

Die UN-R 156 sieht vor, dass der TD durch eigenständige Tests am repräsentativen Fahrzeug[12] prüft, inwiefern die vom Hersteller dokumentierten Maßnahmen umfassend sind und entsprechend implementiert worden sind. Dies sollte ggf. in Kooperation mit dem Hersteller zu erfolgen.

[12] Hier und im Folgenden: Falls der worst case nicht ausreichend an einem Fahrzeug geprüft werden kann, auch an mehreren Fahrzeugen.

Ein Hersteller muss die Beachtung der Cybersicherheits-Anforderungen an die **Software Updates** im konkreten Fahrzeug darstellen können. Das bedeutet:

- Die Authentizität und Integrität der Software-Updates müssen angemessen geschützt werden […] (7.2.1.1.).
- Die RXSWIN (RX Software Identification Number) und die Software Versionen im Fahrzeug müssen gegen unautorisierte Modifikation geschützt werden (7.2.1.2.3.).

3 Allgemeine Verfahrensschritte zur Prüfung

3.1 Allgemeines

Auffälligkeiten, gefundenen Schwachstellen und Abweichungen von den erwarteten Test-(teil-) Ergebnissen sind zu dokumentieren. Ggf. ist der Hersteller zu informieren. Sofern sinnvoll, kann der Test unter mindestens gleichen Bedingungen nach erfolgter Nachbesserung bis zu zweimal wiederholt werden. Der TD entscheidet nach eigenem Ermessen über die Erweiterung des Tests um mögliche bisher nicht betrachtete Risiken, die in diesem Zusammenhang aufgedeckt worden sind, abzuprüfen. Sofern die (Teil-) Prüfung auch dann noch als nicht bestanden zu bewerten ist, ist dies der Genehmigungsbehörde im Prüfbericht mitzuteilen. Die Genehmigungsbehörde prüft dann Auswirkungen auf das eventuell bereits erteilte Zertifikat und wird in der Regel die Genehmigung verweigern.

3.2 Prüfung und Dokumentation

3.2.1 Cybersicherheit

Die Produkttests des TD im Hinblick auf die Cyber-Sicherheit gemäß UN-R 155 und UN-R 156 sollten folgende generischen Verfahrensschritte umfassen:

1) Sichtung der Dokumentation
   - Im Rahmen des Genehmigungsantrags stellt der Hersteller dem TD die notwendige Dokumentation zur Verfügung. Die Dokumentation umfasst mindestens die Risikoanalyse und die im Beschreibungsbogen gemäß Anhang 1 zu den UN-R 155/156 genannten Unterlagen. Der TD prüft die Dokumentation auf Vollständigkeit und Korrektheit und Plausibilität.

2) Definition der Testspezifikation/Erstellung eines Testplans
   - Auf Grundlage der Dokumentation aus Schritt 1, insbesondere der Risikobewertung und Testdokumentation des Herstellers, trifft der TD eine Auswahl an durchzuführenden Funktions- und/oder Sicherheitstests. Hierbei sind die Aspekte aus dem Abschnitt 2.2.2[13] zu berücksichtigen. Um einen gewissen Testumfang sicherzustellen, sollte für jede der in UN-R 155, Annex 5, Tabelle A1 genannten High-Level-Bedrohungsgruppen 4.3.1 bis 4.3.7 ein relevanter Test ausgewählt werden, sofern diese für das zu prüfende Produkt anwendbar sind. Falls hiervon abgewichen wird, ist zu begründen, warum für eine bestimmte Gruppe keine gesonderte Prüfung geplant ist (weil z. B. eine dieser Prüfungen so komplex ist, dass sie mehrere Gruppen abdeckt oder weil das Risiko so untergeordnet ist, dass man die Prüfung – nach Risikoabschätzung durch den TD – auf etwas Anderes konzentriert). Der Technische Dienst entscheidet in eigener Verantwortung, ob er jeweils Funktions- oder Sicherheitstests (im Sinne von Abschnitt 1.1) durchführt.
   - Es sollte eine vorbereitende Schwachstellenrecherche gemäß 2.2.5 durchgeführt werden.
   - Es sind die zu erwartenden Testergebnisse zu definieren.
   - Die Auswahl und Festlegungen der Prüfaspekte (2.2.2) sind zu dokumentieren.

3) Definition der Testumgebung/Infrastruktur
   - Eine geeignete Testumgebung zur Umsetzung der Spezifikation aus Schritt 2 ist vorzubereiten. Es ist zu entscheiden, ob die Tests in eigenen Räumlichkeiten, bei einem geeigneten Auftragnehmer oder beim Hersteller durchgeführt werden.

4) Optional: Test Kick-Off und Whiteboxing
   - Falls erforderlich, werden weitere notwenige Informationen zur Durchführung der Tests (Offenlegung relevanter Design- und Schnittstellen-Informationen zum Prüfobjekt) beim Hersteller eingeholt.

5) Durchführung Funktions-/Sicherheitstests
   - Die Tests werden gemäß Spezifikation/Plan aus Schritt 2 durchgeführt und die Ergebnisse geeignet dokumentiert.

6) Erstellung Prüfbericht
   - Die Testdokumentation des TDs wird in einem Prüfbericht strukturiert gemäß dem vorliegenden Dokument zusammengestellt und dem KBA übermittelt.

3.2.2 Funktionsprüfungen

Sofern nach UN-R 156 reine Funktionsprüfungen ohne Bezug zur Cybersicherheit (gemäß UN-R 156, Abschnitt 7.2) durchgeführt werden, werden diese vom TD analog zu Abschnitt 3.2.1 in geeignetem Umfang spezifiziert, durchgeführt und dokumentiert.

[13] Sofern nicht anders festgelegt, beziehen sich die Referenzen auf Abschnitte dieses Anhangs.

Impressum

Herausgeber:
Kraftfahrt-Bundesamt
Postfach 12 01 53
01002 Dresden

Internet: www.kba.de

Fachliche Auskünfte und Beratung:

Telefon: 0461 316-2600
Telefax: 0461 316-2636
E-Mail: benennungsstelle@kba.de

Erschienen im Januar 2021
Stand: Januar 2021

Druck: Druckzentrum KBA

Bildquelle: KBA/www.shutterstock.com (© Bauer Alexander)

Wir punkten mit Verkehrssicherheit!