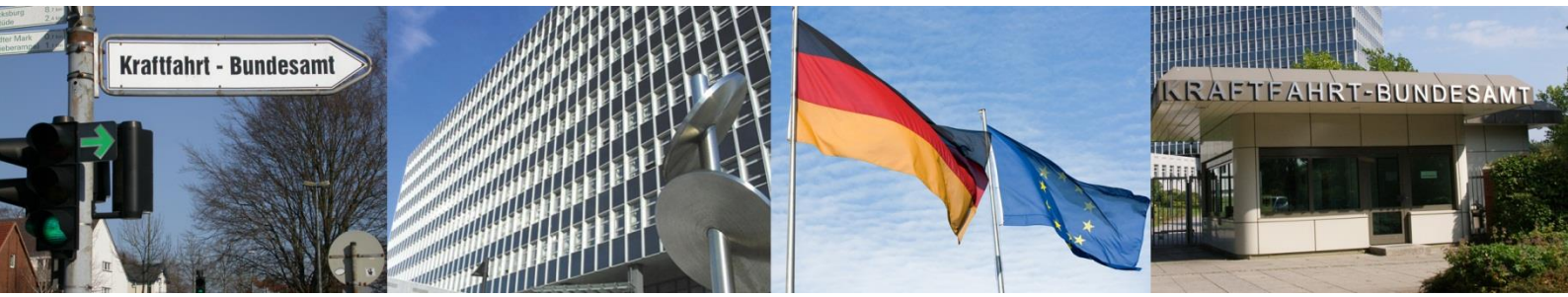
Kraftfahrt-
Bundesamt

Application of the Rules for designation/recognition for technical services (categories A, B, D)

for testing in the context of the

KBA-type approval procedure according to UN-R 155/156

Version: January 2021



Contents

1 Introduction

This document is valid in addition to the Rules for designation/recognition for technical services (categories A, B, D)[1]. It is thus binding for all designated by the KBA technical services (TS) active in this scope.[2]

After consultation with the Technical Committee (AK-T) or its cybersecurity (CS) sub-group, the document will be revised in accordance with any guidance received from the competent UN and/or EU bodies and any experiences made. The respective current version will be published in the Technology Portal of the KBA homepage.

The respective latest UNECE Interpretation Document shall be observed.

The KBA may authorise exemptions. Respective applications should be made in advance wherever possible.

2 Responsibilities

The KBA

- Appoints TS in accordance with its designation rules and this document
- Issues and, if applicable, suspends or withdraws the certificate required by the UN-R on the basis of audit reports and other information
- Issues the type approval
- Organises the exchange of experiences between all interested parties with the objective to further developing the procedure
- Is responsible for communicating with the relevant UN and EU bodies.

The TS designated for the relevant scope

- In general, carries out the testing of the approval object and the CSMS/SUMS. The KBA may, at its sole discretion, carry out additional tests.
- Transfers the relevant information submitted by the manufacturer to the KBA.

[1] Hereinafter, the term ‘designation rules’ will be used instead
[2] Only the German version is binding. Translations are for information only.

The assessed manufacturer[3]

- Grants the necessary access to the premises and information for
    - TS within the surveillance period of 3 years
    - The KBA and authorized by the KBA persons during validity of the certificate and/or type approval
- Provides the TS with the necessary information, documents and records (cf. in particular paragraph B 2.3) (additional submission to the KBA might be omitted, if this is not required by individual request or this does not have direct influence on the validity of certificate or type approval).

3 Definition of terms

Non-conformity: Insufficient compliance with a requirement.

Requirement: Need or expectation that is stated, generally implied or obligatory (EN ISO 9000; please also note the explanatory notes there).

Audit: systematic, independent and documented process for obtaining objective evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled (cf. EN ISO 9000). Within the scope of designation by the KBA, this term is used synonymously with 'assessment' and the like.
Recommendation: See notes to 'should'.

Functionality test: Tests whether the security measures specified by the manufacturer meet their objective (e.g. testing a secure communication protocol regarding its suitability for software update) (cf. also Annex 2).

Process capability: Sufficient capability of a process to meet the objectives defined by regulations, specifications and by the manufacturer with a sufficient probability.

Re-audit: Audit for the purpose of having a certificate renewed for the same scope and immediately following the period of validity of the previous certificate. Such an audit is normally to be carried out during the period of validity of the previous certificate. If more than 90 days have elapsed between the expiry of the previous certificate and the beginning of the audit, the audit time must be the same as for an initial audit.

Security test: Active attempt by a tester to circumvent security measures (e.g. penetration tests) (cf. Annex 2)

[3] Hereinafter, the term 'manufacturer' will be used instead

Stage 1 audit: Audit with the following objectives:
- Evaluation of readiness for the main audit
- Evaluation of documented information
- Identification of site-specific conditions
- Collection of information on the scope of the CSMS/SUMS
- Refinement of planning of the main audit, determination of resources required for the main audit

For details, cf. EN ISO/IEC 17021-1

Pre-audit: Optional inventory and document review on site, allowing the early detection of potential weaknesses in the documents and the implementation of the system. It is comparable to a dress rehearsal, but is generally less comprehensive than the main audit.

Witnessing: Assessment of the performance of testers/auditors by the KBA or a body commissioned by it. The witness-assessor generally does not directly influence on the activities of the tester/auditor.

In this document:
- 'must', 'shall', 'is to' or similar phrases denote a binding requirement.
- 'should' denotes an accepted way of complying with the requirements of an UN regulation or of the designation rules. A TS may use at least equivalent options, provided that evidence of this can be provided to the KBA.
- 'can', 'may' denotes a possibility (option for implementation).

Abbreviations:

AS	Authorised signatory
CR	Catalogue of requirements
CS(MS)	Cybersecurity (management system)
ISMS	Information security management system
KBA	Kraftfahrt-Bundesamt (Federal Motor Transport Authority)
QM	Quality management
RASIC	Responsible, accountable, supportive, informed, consulted
STEM	Science, technology, engineering, mathematics
SU	Software update
TAP	Type approval procedure
TS	Technical Services
UN-R	UNECE Regulation

Part A Designation of technical services

A 1 General

Designations for testing or auditing within the scope of CS/SU are made on application in categories A, B and/or D.

They are made in a new Scope (Prüfgebiet) 14, Hence the sample size for assessments increases.

14	Information technology/artificial intelligence/cybersecurity
14-01	Cybersecurity/software update (product testing)
14-01-01	UN-R 155
14-01-02	UN-R 156
14-10	Testing of management systems in the Scope (Prüfgebiet)
14-10-01	UN-R 155
14-10-02	UN-R 156

Technical Services may only be designated for CS and/or SU testing/auditing if they are also designated for testing of whole vehicles within the scope of the respective CS/SU legal act and/or if they can demonstrate close relations to a TS designated for ‘whole vehicle’ (see No. A 2).

The designation for CSMS/SUMS can only be made if the TS is also designated for product tests in the respective scope. Thus, for instance, designation for 14-01-01 is a prerequisite for designation in 14-10-01.

A 2 Requirements for the documentation of the QM system

QM documents or extensions to existing QM documents of the TS:

- Procedures for testing/auditing in accordance with UN-R 155/156
- Requirements for personnel involved
- Regulations for handling confidential information (particularly CS/SU-relevant information)
- Where needed: documented interpretation of UN-R and KBA requirements.

To a reasonable extent, the relevant information must, on request, be made available to the client.

A 3 Requirements for personnel

The requirements of the designation rules shall have effect, in the following specification and/or with the following additions.

In general, the authorised signatory (AS) is classed in experience category 4 (see designation rules) for both product and management system testing. The relevant professional experience should not date back to more than 5 years.

The KBA may, on application, grant exemptions, but reserves the right to intensify witnessing in such cases.

A 3.1 Personnel for product tests

Requirements for an AS:

- Academic degree in accordance with the designation rules (STEM programs at least in part including knowledge of the relevant area of application are particularly relevant)
- In-depth knowledge of testing according to UN-R 155/156 within the meaning of Section B 3 (e.g. penetration, fuzz, side-channel, functionality tests)
- Knowledge of the whole vehicle following the relevant content of the KBA framework training program for AS for whole vehicles (training in a TS designated for testing whole vehicles)
- Knowledge of and skills in applying (automotive) methods of risk analysis
- Knowledge of and skills in auditing management systems in the automotive industry (preferably including CSMS/SUMS).

A 3.2 Personnel for evaluation of management systems

Requirements for an AS:

- Academic degree in accordance with the designation rules (STEM programs at least in part including knowledge of the relevant area of application are particularly relevant)
- Expertise according to ISO/IEC 27001 with focus on cybersecurity in the automotive industry, ISO 21262 with focus on cybersecurity or at least equivalent relevant requirements
- Successful completion of training as an auditor of management systems (comparable to EOQ)
- At least 1 year’s (3 audits’) experience as an auditor in the automotive industry
- Knowledge of and skills in applying (automotive) methods of risk analysis
- Knowledge of the whole vehicle with regard to interaction of systems and components.

Furthermore, the ‘Requirements for personnel of a technical service for auditing a CSMS according to UN-R 155 and 156’ (see Annex 1) shall have effect.

Where the requirements under A 3.1 and/or A 3.2 are not met, the following will be accepted:

- The AS himself/herself has at least one year’s personal experience of selecting, carrying out/supervising and evaluating the relevant test procedures (participation in relevant panels will be taken into account), and
- The AS has provided evidence of basic knowledge of the interactions and the potential risks of systems and components in a whole vehicle. Such evidence was provided to the head of a TS designated for ‘whole vehicle’ or to an AS authorised by that head of TS and
- The AS is being supported by relevant technical experts in the areas where there is a lack of knowledge/skills.
- Knowledge of the relevant area of application may have been acquired after completion of the academic degree.

A 3.3 Maintaining competence

The AS for product testing and the AS for evaluation of the management system, all auditors used within this scope as well as technical experts shall take part in an exchange of experiences in applying UN-R 155/156 at least once a year. At least once every 3 years, experiences within their own TS shall also be exchanged. This exchange of experiences may be carried out along with other exchanges of experiences in the TS; however, it must address the issues of auditing/homologation testing within the area of CS/SU for a proportion of time to be determined by the head of the TS.

It is desirable, where such contracts exist, that they take part in relevant audits at least once a year (with the AS for product testing and the audit team leaders also taking part in planning and carrying out product tests and the annual document review).

The KBA and the head of the TS may make further arrangements.

The head of the TS shall document the requirements for all personnel involved in his/her QM system.

A 4 Designation procedure

A 4.1 General

The KBA may consult technical experts for its assessments. The names and, on request, places of work of the technical experts will be communicated to the TS. Assessors and technical experts may, in individual cases and with sufficient reasons, be rejected by the TS.

A 4.2 First designation in the Scope (Prüfgebiet)

The decision on the designation for the relevant Subscope (Prüfumfang) will be made following an office and witness assessments. It may be made provisionally after the office assessment, subject to successful witnessing. The KBA will decide on the scope of any measures in the event of extensions in the Scope (Prüfgebiet) 14 at its sole discretion.

Reasonable consideration will be given to accreditations for tests under UN-R 155/156 and/or ISO 21434 and other accreditations; these may lead to a shorter inspection.

A 4.3 Surveillance

Surveillance in the Scope (Prüfgebiet) 14 will be performed in accordance with the general designation rules.

In case of designation for Subscope (Prüfumfang) 14-10, there will also be at least 1 witness assessment in the course of the surveillance period (2.5 years), if relevant audits take place. To that end, the TS shall notify the KBA no later than 4 weeks before any such audit.

Part B Tests by the TS as part of the TAP

B 1 General

The objective of the tests/audits is to demonstrate that

- The installed system is suitable, adequate and effective, in particular, that the installed processes are sufficiently capable[4] of implementing the objectives and functions specified by the UN-R and the manufacturer;
- There is no significant risk to security, the environment, or health within the scope of UN-R 155/156;
- The information provided by the manufacturer has been verified;
- The manufacturer has implemented its documented measures in a satisfactory manner.

The manufacturer is expected to develop and implement risk analyses and other analyses and measures/products in accordance with good engineering practice. Reasons must be given for any divergence from such practice. In that case, the TS will evaluate the appropriateness of such divergence and note this in the report. This applies, in particular, to cryptographic methods.

If in case of lack of full competence of the AS, technical experts have been called on, such experts shall sign for the accuracy of the relevant partial results for which their expertise was used in the internal files of the TS.

In that case, the assessment by the person signing the test/audit report must not be more favourable than that by the respective technical experts. Any exceptions to this rule must be justified in the report or in the covering letter to the KBA, stating the dissenting opinions.

The KBA and the TS store documents and data of the manufacturer only if this is absolutely necessary and only for the necessary time in an appropriately safeguarded environment. If not defined otherwise in this document, the retention periods as defined in the respective KBA Recommendations should be applied. TS and the KBA are allowed to open data and documents to third parties if there is a legitimate interest and if the manufacturer has not explicitly required confidentiality. The KBA or the TS inform the manufacturer prior to publishing. Such a publishing shall be recorded.

[4] Mathematical-statistical evidence is not required.

B 2 Auditing and other assessment of the CS and SU management system (CSMS/SUMS)

B 2.1 General

In general, the KBA will only issue certificates for CSMS and SUMS according to UN-R 155/156 to manufacturers of whole vehicles within the scope of the respective UN-R. If other manufacturers apply for an audit for the purpose of obtaining such a certificate, it is strongly recommended that the KBA be consulted before such a contract is accepted.

As a general rule, for each manufacturer, the complete relevant management system must be audited and evaluated.

Unless otherwise provided in this document, it is recommended that the general requirements of ISO/IEC 27006 in application to UN-R 155/156 be applied.

Alongside the reports listed under No. B 3, the TS shall submit to the KBA designation body information on all facts relevant to a type approval according to UN-R 155/156 of which they have become aware.

B 2.2 Scope and type of first test and monitoring

Prior to the first decision on a certificate, and at least every 3 years thereafter (re-audit) (if the holder of the type approval is interested in the continued validity of the type approval), an on-site audit (main audit) must be carried out. Thereafter, there shall be at least a document review every 12 ± 1 months.

If considered necessary by the TS or the KBA on an ad hoc basis, further on-site audits (e.g. Stage-1 audits, follow-up audits, special audits) and document reviews may be carried out. More than one pre-audit per application for an initial certificate or for extension of the certificate is considered to be consultation and thus inacceptable.

Between audits, the TS shall evaluate any information with relevance to the certificate of which it becomes aware. The manufacturer shall be required by the TS to provide all relevant information. The TS shall derive from this any additional monitoring measures that may be required and shall notify the KBA in the event that this is of major significance to the continued validity of the certificate or the type approval.

B 2.3 Document review

B 2.3.1 General

Documents and records must be suitable for ensuring and demonstrating the capability of the relevant manufacturer’s processes.

Manufacturer, TS and the KBA agree on appropriate communication channels. The document review may be carried out on site, if appropriate. In that event, no more than one third of the time for document review must be allocated to the on-site audit time according to No. B 2.4 (except for parts appertaining to the risk analysis).

The annual document review between on-site audits may be limited to documents marked (*) and other documents with major changes.

Documented information, software and other audit evidence in possession of the manufacturer shall be left in its possession; no copies shall be made. The auditor's records must be sufficiently informative to describe the facts and to document the objective evidence. In exceptional cases, originals or copies may be requested from the approval authority. For that reason, the assessed organisations must be required to keep essential documents for no less than 12 months following the audit.

B 2.3.2 Minimum scope of the document review according to UN-R 155

The organisation to be assessed shall submit at least the following documents and possibly existing records to the TS:

- Completed KBA catalogue of requirements[5] and referenced documents, if applicable
- Required documents[6] according to UN-R 155 (cf. Annex 1 to the UN-R)
- Description of the CSMS containing at least the following:
    - General principles
    - If applicable, exclusions with respective justification
    - Project-related cybersecurity management
    - * Continuous cybersecurity activities
    - Risk assessment methods
    - Cybersecurity management in the product life cycle (design, development, production, operation and maintenance, disposal)
    - If applicable, measures for ensuring CS in respect of suppliers/service providers/subcontractors
    - CoP and market surveillance in relation to CS
    - Information management with respect to CS (internal, external)
- General process landscape of the manufacturer, showing cybersecurity aspects
- Organisation charts showing cybersecurity aspects
- Description of roles in CSMS processes (RASIC)
- Risk analysis with associated initial and test information
- * If applicable, a list of CSMS-relevant suppliers/service providers/subcontractors with their respective duties and responsibilities and an assessment of the relevant risks
- Procedures, test plans, test instructions and any other documents related to CSMS

[5] On prior arrangement, the KBA will also accept at least equivalent catalogues of requirements and/or reports.

[6] If the contents of the documents form a subset of further documents listed in this section, a reference to the documentation with appropriate notes will be sufficient.

- * Results of tests/audits carried out (overview)
- * Records related to ensuring CoP and to market surveillance in respect of CS, in particular to any CS incidents (including attempted attacks)
- * Records regarding enquiries from external parties regarding CS

B 2.3.3 Minimum scope of the document review according to UN-R 156

The organisation to be assessed shall submit at least the following documents and possibly existing records to the TS:

- Completed KBA catalogue of requirements[5] and referenced documents
- Required documents according to UNECE-R 156 (cf. Annex 1 to the UN-R)
- Description of the SUMS containing at least the following:
    - General principles
    - If applicable, exclusions with respective justification
    - Risk assessment methods (including security risk analysis)
    - SU management in the product life cycle (design, development, production, operation and maintenance, disposal)
    - Identification and reporting capabilities in relation to the software installed and activated in the vehicle
    - If applicable, a list of SUMS-relevant suppliers/service providers/subcontractors with their respective duties and responsibilities, including an assessment of the relevant risk
    - CoP and market surveillance in relation to SU
    - Information management with respect to SU (internal, external)
- General process landscape of the manufacturer, showing SUMS aspects
- Organisation charts showing SU aspects
- Description of roles in SUMS processes (RASIC)
- Risk analysis regarding SUMS with associated initial and test information
- * If applicable, a list of SU-relevant suppliers/service providers/subcontractors/other relevant parties with their respective duties and responsibilities and an assessment of the relevant risk
- Procedures, test plans, test instructions and any other documents related to the SUMS
- * Results of tests/audits carried out (overview)
- * Records related to ensuring CoP and to market surveillance in respect of SU, in particular to any SU incidents (including attempted attacks)
- * Records of enquiries from external parties regarding SU

B 2.4 Requirements for the on-site audit

The regulations according to ISO/IEC 27006 shall have effect, where applicable. A formal Stage-1 audit may be carried out, but is not required. Nevertheless, the content of Stage 1 must be covered.

The on-site audit shall be preceded by a document review.

The KBA recommends using the methodology according to ISO/IEC 27006 for calculating the audit time, having regard to the following constraints:

- The baseline shall be the values given in the table in ISO/IEC 27006, applied to at least all personnel and other managers relevant to the scope to be audited (e.g. from development, product testing, auditors etc.) and managers of the departments on all relevant sites including the headquarters (e.g. quality planning, production, purchasing etc.). It is recommended to assume for calculation approximately 7 per cent of the total number of employees within the scope of the certificate. The audit time will be calculated in agreement with the audit team leader (authorised signatory) shall decide in accordance with TS procedures. Given that the CSMS/SUMS covers only parts of an ISMS, a ‘normal’ amount of work and ‘medium complexity’ according to ISO/IEC 27006 can be assumed.
- The amount of time thus determined is to be increased according to the results of the document review, experience of previous audits, the complexity of the products and/or processes, the risk assessment, time for translation and the like. For the same reason, it may be reduced by a maximum of 20 per cent (e.g. no development responsibilities, simple products/processes, experience of previous audits).
- For re-audits, 2/3 of the calculated value is to be assumed (cf. ‘Definition of terms’).
- No less than 70 per cent of the time thus calculated, but no less than 32 hours (for re-audits: 24 hours) must be audited on-site. In case of justified other calculation, the prior agreement of the KBA must be obtained. This guideline takes into account up to 1 hour for auditors’ time and daily summaries/other co-ordination per day (on the final day: 2 hours) plus non-productive (e.g. transit) time up to a maximum of 1 hour/day. Breaks and other (e.g. travel) times must be planned for in addition.

Random sample auditing of product tests by the manufacturer forms part of the audit (as evidence of testing competence) At the TS’s discretion, this time can also be accounted for as part of homologation testing. It is suggested to plan 4 hours for this.

In case of several sites, the methodology according to IAF MD1 should be applied.

Splitting the audit team for different audit phases shall be permissible only if the auditor and/or the (partial) audit team in each audit phase are sufficiently competent to assess CS/SU and management systems (see A 3, ‘Requirements for personnel’).

ll relevant requirements according to the KBA catalogue of requirements[5] must be assessed on the basis of the review of documents and records, interviews, and observation of actual processes and tests. In case of re-audits, the results of tests/audits in the past 3 years shall be taken into account.

The duplication of auditing or testing is to be avoided. The TS shall decide to what extent other certificates (e.g. certifications according to ISO 21434 or UN-R 155/156) can be accepted, thus reducing the audit time. Prior co-ordination with the KBA is recommended. The decision and its justification must be recorded in the audit or test report.

The auditing of the post-production phase/end-of-life phase/market surveillance relates only to those factors, which are in the manufacturer's control, and will focus on the relevant part of the risk analysis and the measures resulting therefrom (including at external sites, such as service centres owned or otherwise supervised by the manufacturer).

Suppliers, service providers and the like will only be included in the audit in relation to the protection of the interface by the manufacturer.

B 2.5 Classification of findings

The classification of the results will be done in accordance with the requirements of ISO/IEC 27006.

Findings can result from the document review and the on-site audit. This classification is also to be followed in assessing other information.

The classification distinguishes:

- Positive findings
- Opportunity for improvement
- Minor non-conformity
- Major non-conformity

Positive finding: Requirements are met beyond the extent to be expected.

Opportunity for improvement: There is potential for improvement, while the requirements are generally met.

Minor non-conformity:
- A deficiency in complying with a requirement which does not compromise the ability of the management system to achieve the intended results.
- An opportunity for improvement that has not been analysed results in a minor non-conformity with respect to the improvement process.

Minor non-conformities not completed in due time result in a suspension procedure. If the number of minor non-conformities suggests a breakdown of the management system, this will result in the same consequences as a major non-conformity.

Major non-conformity:
Non-compliance with a requirement which does compromise the ability of a management system to achieve the intended results. This must be assumed e.g. in the following cases:

- Serious doubt that there is effective process control or that products and/or services meet the specified requirements
- Serious doubts as to the quality of the risk analysis, of the measures initiated as a result, as to test planning, as to tests and as to decisions about meeting the requirements (among other things, in respect of achieving an acceptable risk)
- Product tests repeatedly yield negative results with similar root-causes
- The holder of the type approval/applicant fails to comply with the provisions of the UN-R, other relevant legal acts and/or the approval and fails to make adequate corrections and to take corrective measures without undue delay.
- A repeatedly observed non-conformity regarding the effectiveness of corrective measures in the past 5 years
- Other serious violations of approval-relevant requirements.

Major non-conformities must be promptly closed by an on-site follow-up audit. This on-site audit will be scheduled for a date no later than 90 days after completion of the main audit. Major non-conformities impede the issuance of the certificate. If they are identified during the term of validity of the certificate and if they are not remedied in due time, they will entail the suspension of the certificate (or of a part of the certificate, at the KBA's discretion).

For minor non-conformities to be closed, at least a programme of measures must have been accepted by the TS. The effectiveness of the measures must be verified at the next audit.

The classification will be decided by the audit team leader, i.e. the person signing the audit report. If technical experts are used, No. B 1 must be observed.

B 2.6 Documents to be submitted to the KBA

Following the on-site audit and the annual document review between regular audits, the TS shall submit the following documents to the KBA designation body:

- Report according to ISO/IEC 27006 regarding compliance with the requirements of UN-R 155/156. The report must state any peculiarities of the audit or the document review such as taking into account other certificates, the exclusion of requirements etc., giving justification. The completed KBA catalogue of requirements[7] with its associated checklists and the assessment reports must be attached to the report as annexes.[5]
- The annual report of the manufacturer about its monitoring activities (only for UN-R 155) and a summarising evaluation of all such reports and information submitted by the manufacturer during the past surveillance period (only in case of annual document review)

[7] May be omitted in case of document review.

- Evidence of a quality check of the report according to the TS's procedures (by at least a CS and MS expert who did not attended the audit, wherever possible)
- List of checked documents[8]
- List of objective pieces of evidence.[8]

The report must be submitted immediately if and when it contains a positive recommendation to issue a certificate and all major non-conformities have been closed (minor non-conformities may still be open and/or need not have been definitively assessed as to the effectiveness of the measures initiated).

The TS must inform the KBA without undue delay if it gets information which can influence the validity of the certificate or the approval. The information by the TS does not replace the obligation of the manufacturer to inform the KBA directly in such situations.

B 3 Product test

B 3.1 General requirements

- As well as the practical test of the product, the test includes verifying the associated documentation (e.g. completeness of risk analysis and appropriateness of the conclusions drawn). The practical part includes an assessment of whether the measures planned by the manufacturer achieve the minimum security objective and the required range of functions.
- At least 1 practical test per UN-R must be carried out/supervised by the TS. The scope and contents of the tests should be planned on the basis of:
  - The risk analysis and the worst-case scenario derived from it, and
  - The security objective defined by the manufacturer (if applicable, also in the post-production phase), and
  - The minimum security objective required and the range of functions as required by the UN-R, and
  - The recommendations in Annex 2

  Depending on the test result, the competence of the tester (where the test is being supervised), etc., further tests will be carried out/supervised by the TS. The tests shall focus on significant risks. The worst-case scenario may require testing on different vehicles.
- The minimum security objective to be expected will result from the relevant UN-R and, particularly during the transition period of the introduction of UN-R 155, must contribute to meeting the general requirement to avoid significant risks to safety, environment, and health. Further specifications will be made at a later date as part of the exchange of experience.
- In choosing tests, as well as the vehicle the back-end should be taken into account.

[8] Unless already shown in the completed catalogue of requirements.

- Significant claims by the manufacturer, such as the claim that a component is not updateable or that an update does not affect other parts/systems of the vehicle, must be verified.
- Where the TS has the test equipment required, the test should be carried out in the TS's own laboratory environment. If appropriate, the manufacturer should assist with the testing (e.g. by providing analysis tools).
- Supervision may be limited to essential phases (e.g. risk analysis, hardware and software used, experimental set-up, partial results, checking records). Where possible, supervision at the manufacturer's premises should also be used to assess testing competence as part of the CSMS/SUMS audit (suitable resources, competent execution, etc.). The supervising TS will define the guidelines for the type of test, use of specific equipment, creation of specific test environments, attack method and target, the vehicle, etc.
- Where tests are supervised and/or third-party test equipment is used, the integrity of the hardware and software used must be ensured in a reproducible manner. The reproducibility of tests must be ensured for a period of at least 10 years after production is definitely discontinued (e.g. by 'sealing' the software).

Notes for carrying out product tests are attached to this document as Annex 2.

If technical experts are to be involved, No. B 1 must be observed.

B 3.2 Documents to be submitted to the KBA

The documentation (the test report) must meet the requirements of the designation rules, in particular of annex 5, and in addition include at least the following:

- Test plan with justification (analogous to the requirements for the manufacturer's test plan; see Annex 2, No. 2.2)
- The expected test results (especially if the UN-R does not contain detailed specifications)
- The actual test results
- Justification of any deviations accepted (including 'gaps' in the risk analysis and the like)
- Peculiarities such as for example the use of hardware and software for testing that is not the property of the TS, and measures for ensuring integrity.

The final statement must be based on statements regarding the foregoing.

Annex 1

Requirements for personnel of a technical service for the auditing of a CSMS in accordance with UN R 155 and 156

ISO/IEC ISO 17021-1:2015 provides general principles for certification of a management system and shall be considered as requirement for technical services. For the implementation of UN-R 155 and 156 by technical services, consideration of ISO/IEC 27006, applied for automotive cybersecurity, is suggested for definition of requirements for auditors. Topics for the certification of cybersecurity management systems can, however, be adopted by vehicle manufacturers.

In this annex, the requirements of ISO/IEC ISO 17021-1 and ISO/IEC ISO 27006 are presented as a basis for the roles of a technical service. A detailed list of requirements can be found in the following tables, where the necessary roles and their competences as well as the required knowledge of an audit team are described.

The abbreviations used for the certification functions are used as followed:

AR (Application Reviewer):	Review of the application to define, in agreement with the lead auditor, the required competence of the audit team, select the members and identify the necessary audit time.
RR (Report Reviewer):	Review of audit reports and proposal for certification.
LA (lead auditor):	Planning of the audit Auditing and management of the audit team Finalisation of the audit report (signature)

1 General requirements

Function	Knowledge and skills		Reference to standards for LA
	ISO/IEC ISO 17021-1	ISO/IEC 27006	
RR, LA		Knowledge of information security management, terminology, principles, practices and techniques	ISO/IEC 27006 7.1.2.1.2
LA	Knowledge of business management practices	Knowledge of business management practices	ISO/IEC 27006 7.1.2.1.4 ISO 17021-1 A.2.1
RR, LA	Knowledge of audit principles, practices and techniques		ISO/IEC 17021-1 A.2.2
AR, RR, LA	Knowledge of specific management system standards and normative documents	Knowledge of information/security management system standards and normative documents	ISO/IEC 27006 7.1.2.1.3 ISO/IEC 17021-1 A.2.3
AR, RR, LA	Knowledge of certification body's processes		ISO/IEC 17021-1 A.2.4
AR, LA, (RR durch ISO 27006)	Knowledge of the customer´s products, processes and organisation	Knowledge of the customer´s products, processes and organisation	ISO/IEC 27006 7.1.2.1.6 ISO/IEC 17021-1 A.2.6
LA	Language skills appropriate to all levels within the client organisation		ISO/IEC 17021-1 A.2.7
LA	Note-taking and report writing skills		ISO/IEC 17021-1 A.2.8
LA	Presentation skills		ISO/IEC 17021-1 A.2.9
LA	Interviewing skills		ISO/IEC 17021-1 A.2.10
LA	Audit management skills		ISO/IEC 17021-1 A.2.11

2 Special knowledge oft he audit team

Due to the fact that the mentioned requirements are largely generic, it is necessary to specify these requirements. With reference to ISO/IEC 27006, ISO/IEC ISO 27002 and ISO 21434, an auditor or a team of auditors shall have knowledge in the following areas:

Subject area	Subject	Base
CSMS in general	Organisation Governance Compliance; Data Protection (Privacy), intellectual property; ISMS	UN-R 155 ISO 27001 ISO 27002 ISO 21434 DSGVO
Cybersecurity Management	Asset management security goals Incident management Vulnerability management Project-related cybersecurity management Handling of external service providers Ongoing cybersecurity activities	UN-R 155 ISO 21434
Product life cycle	Concept phase Development phase Production phase Post production phase	UN-R 155 ISO 21434
Threat and risk assessment	Asset identification Threat identification Impact analysis Attack path analysis Probability analysis Evaluation, treatment	UN-R 155 ISO 21434
Threats	Back-End Server Internal vehicle communication External vehicle communication Update procedure Unintended human actions Code vulnerabilities Physical manipulation	UN-R 155
Cybersecurity Test	Penetration testing Fuzz testing Static code analysis Interface testing Vulnerability scanning Simulation Hardware	UN-R 155 ISO 21434

Subject area	Subject	Base
Cybersecurity	Vulnerabilities of cryptography Communication security Integrity Confidentiality Interaction	UN-R 155 ISO 21434

Requirements of UN-R 156 are to be applied adequately.

Annex 2

Notes on product tests and vulnerability analyses in accordance with UN-R 155 and UN-R 156 Guidance[9]

Annex to the KBA document
"Application of the Designation Rules for technical services to tests according to UN-R 155/156"
(Part B Section 3)

1 Introduction and definitions

1.1 Functionality and security tests

This document covers two kinds of tests; for ease of reference, these will be discussed separately. They involve, on the one hand, testing the functions (functionality tests) and, on the other hand, testing for cybersecurity (security tests). Functionality tests confirm that the (functional) requirements are met, while security tests confirm that IT security objectives are met.

Security tests are those which simulate actual and current attacks, so as to identify possible risks to the cybersecurity objectives. It must be tested whether an attacker exploiting an (unknown, as the case may be) vulnerability of the system (here: from the vehicle up to the back-end infrastructure) can gain unauthorised access to the system's data or resources.

Unlike tests for functional safety, security tests within the meaning of UN-R 155/156 do not test/are not developed for natural, heuristic errors (such as software errors, (E/E-) component failures, configuration errors, etc.), but for intentional attacks which may involve complex attack vectors and forced system states.

However, any security measures implemented, such as cryptographic protocols, can also be subjected to pure functionality tests (not security tests under this definition). Here, it is first tested whether a security mechanism functions according to specifications without trying to actively circumvent it.

[9] This guidance including its recommendations was developed by the Federal Office for Information Security in collaboration with the KBA (Federal Motor Transport Authority) and approved by the KBA as an annex of this document.

1.2 Correlation UN-R 155 with 156 (cybersecurity)

To begin, it must be noted that the two UN Regulations are independent of each other; accordingly, products may be approved according to one or the other.

Ensuring cybersecurity is the inherent purpose of UN-R 155. In addition, UN-R 156 contains requirements for cybersecurity (e.g., 7.1.3. 'Security [...]'), which can either be taken into account in the context of a test under UN-R 155[10] or must be dealt with by a separate security test for the type approval under UN-R 156. Where the testing/type approval for both regulations is done at the same time, TS and approval authority[11] are advised to combine the test plans for both regulations under this aspect.

1.3 Further documents

State-of-the-art product development produces a large number of useful documents (e.g., in future, work products under ISO/SAE 21434 etc.), which should be used in the type approval procedure for targeted and efficient testing.

Any other documents required will be specified in the KBA's Sanctioned Interpretations.

2 Aspects of cybersecurity testing

2.1 Assessment of manufacturer´s documentation

Tests by the technical service are based on the risk analysis and the manufacturer's test documentation.

The documentation should contain a test plan (with justification), the expected test results, and the actual test results.

The test plan should include a description of the test scenarios and tests carried out for each interface/component of the vehicle considered. It should also note any interdependence between tests (e.g. Test B requires the results of Test A).

The TS will assess the completeness of the test plan and the conformity of actual to expected results of the manufacturer's tests. See also Section 3.

[10] This may be as an extension of the scope of the threats to/the vulnerability of update processes (cf. Table A1, Annex 5, UN-R 155).

[11] Hereinafter, the term 'TS' will always also refer to the approval authority, except where expressly stated otherwise.

2.2 Practical tests by the TS

The following aspects must be clarified before tests are carried out by the TS:

2.2.1 Own tests

Will testing only involve reproducing the manufacturers' tests or will it also involve performing/supervising (functionality or security) tests of the TS's own design?

Recommendation

Functionality and security tests designed by the TS itself should be performed, especially where gaps are apparent in the test plan.

2.2.2 Scope an coverage of testing

On how many and which of the vehicle's interfaces will tests be reproduced or performed/supervised by the TS?

Recommendation

As a preliminary approach, taking into account the resources (particularly the time) available, a quantity of the vehicle's interfaces should be individually selected and tested by the TS. In selecting them, the risk analysis should be taken into account. In the medium term, the (minimum number of) interfaces/components to be tested should be defined in a best practice guideline.

Will testing cover only external interfaces of the vehicle or will it also cover internal components and interfaces (not directly accessible externally)?

Recommendation

When making the above selection, external interfaces should be given priority, as these are expected to be at a higher risk. In certain cases (if security is particularly dependent on an internal component), random samples of internal components may also be tested.

See also Section 3.

2.2.3 Test environment

In what environment will the tests be performed?

Options

- At the manufacturer's premises. The TS supervises the test.
- At the TS's premises. The manufacturer provides a suitable test object and suitable test equipment.
- At the TS's premises. The manufacturer provides a suitable test object. The TS uses only its own test equipment or test equipment hired by itself.

Recommendation

Where the TS has the test equipment required, the test should be carried out in the TS's own laboratory environment.

The responsibility for the suitability [...] of the equipment and methods used for testing lies solely with the TS, whether or not the TS is the owner of such equipment and methods (cf. ISO/IEC 17020:2012).

Applicable standards for creating confidence in the work of laboratories/inspection bodies and requirements of the same (e.g., ISO/IEC 17020, ISO/IEC 17025) should be appropriately interpreted for and applied to the special requirements of cybersecurity. This is justified by the active nature of the 'error source', which can here occur intentionally – in the worst case, during testing of the systems.

Where testing is supervised and/or third-party test equipment is used, the integrity, the correct configuration and, as the case may be, the correct calibration of the test hardware and software used must therefore be ensured in a reproducible manner. The reproducibility of the test must be ensured for a period of at least 10 years after production is definitely discontinued (including documentation and, if appropriate, by 'sealing' the test hardware and software used).

2.2.4 Level of attack (for security tests)

What level of attack is assumed?

The level of attack is determined e.g. by the following factors:

- Time available
- Expertise of the attacker
- Available knowledge about the test object (white-box, grey-box, black-box testing)
- Available tools (tools available commercially, special tools, manufacturer's tools, self-developed tools...)

Options

- A general minimum level is set.
- The level of attack is set for individual cases depending on the risk analysis carried out by the manufacturer or the risk assessment carried out by the TS itself.

Recommendation

In general, the greater the risk from a component/interface under consideration is judged to be, the higher the assumed level of attack to be selected. As a rule, white-box or grey-box tests should be performed, as the relevant manufacturer's documentation should be available.

2.2.5 Preparatory analyses (for security tests)

Which preparatory analyses will be carried out?

Options

- Only security tests already performed by the manufacturer will be reproduced.
- A number of pre-defined 'standard tests' (brute-force attacks, fuzzing, etc.) will be performed.
- Vulnerabilities of the test object are researched using publicly accessible information sources/databases or, if applicable, the TS's own databases. If positive results are found, the relevant attacks will be performed if they do not exceed the set level of attack.
- On the basis of available design documents and functional specifications, interfaces potentially vulnerable to attack are identified. Individually specified attempted attacks (at a given level of attack) will then be carried out on those interfaces by an experienced penetration tester.

Recommendation

Independent research into known vulnerabilities should be carried out. Individually specified penetration tests by the TS are strongly recommended.

2.3 Requirements under UN-R 156

UN-R 156 provides that the TS, using independent tests on a representative vehicle,[12] verifies to what extent the measures documented by the manufacturer are comprehensive and have been implemented accordingly. This should, if possible, be done in co-operation with the manufacturer.

[12] Here and hereinafter: or on several vehicles, if the worst-case scenario cannot sufficiently be tested on one vehicle.

A manufacturer must be able to demonstrate compliance of the **software updates** with the cybersecurity requirements on a specific vehicle. This means:

- The authenticity and integrity of software updates must be reasonably protected [...] (UN-R 156, 7.2.1.1.).
- The RXSWIN (RX software identification number) and software versions on a vehicle must be protected against unauthorised modification (UN-R 156, 7.2.1.2.3.).

3 General procedural steps for testing

3.1 General

Any abnormalities, vulnerabilities identified, and deviations from the expected (partial) test results must be documented. If necessary, the manufacturer must be notified. Where appropriate, following rectification, the test may be repeated up to two times, under at least equivalent conditions. The TS shall decide, at its own discretion, whether to extend testing to cover any potential risks not previously considered and identified in this context. If the (partial) test even then cannot be recognised as passed, the approval authority must be notified of this in the test report. The approval authority will then evaluate the impact on the – possibly already issued – certificate and, as a rule, refuse the approval.

3.2 Testing and documentation

3.2.1 Cybersecurity

The product tests by the TS regarding cybersecurity according to UN-R 155 and UN-R 156 should include the following generic procedural steps:

1) Review of documentation
   - As part of the application for the approval, the manufacturer will provide the TS with the requisite documentation. This documentation will contain at least the risk analysis and the documents mentioned in the information document according to Annex 1 to UN-R 155/156. The TS is to check the documentation for completeness and accuracy and plausibility.

2) Definition of test specifications, preparation of a test plan
   - On the basis of the documentation reviewed in step 1, in particular the manufacturer's risk analysis and test documentation, the TS is to make a selection of functionality and/or security tests to be carried out. The aspects covered in Section 2.2.2[13] must be taken into account here. To ensure a certain scope of testing, one relevant test should be selected for each of the high-level treat groups 4.3.1 to 4.3.7 mentioned in UN-R 155, Annex 5, Table A1, if these are applicable to the product to be tested. If this is not observed, i.e., if no separate test is planned for a specific group, this must be justified (e.g., because one of these tests is so complex as to cover several groups, or because the risk is so secondary that testing – following a risk assessment by the TS – is to focus on something else). The TS shall decide in each case, at its own responsibility, whether to carry out functionality or security tests (within the meaning of Section 1.1).
   - Preparatory research of vulnerabilities according to 2.2.5 should be carried out.
   - The expected test results must be defined.
   - The selection and specifications of the test aspects (2.2.2) must be documented.

3) Definition of the test environment/infrastructure
   - A test environment suitable for the implementation of the specifications from step 2 must be prepared. It must be decided whether the tests will be carried out in the TS's own premises, at a suitable subcontractor's premises, or at the manufacturer's premises.

4) Optional: Test kick-off and white-boxing
   - If necessary, further information regarding the performance of the test (disclosure of relevant design and interface information for the test object) will be requested from the manufacturer.

5) Performing functionality and security tests
   - The tests are carried out according to the specifications/plan from step 2, and their results are appropriately documented.

6) Preparing the test report
   - The TS's test documentation shall be compiled in a test report in a structured manner according to the document 'Application of the Designation Rules' and submitted to the KBA.

3.2.2 Functionality tests

If pure functionality tests are carried out under UN-R 156 without reference to cybersecurity (according to UN-R 156, Section 7.2), these shall be specified, performed, and documented to a suitable extent by the TS analogously to Section 3.2.1.

[13] If not defined otherwise, references are given to paragraphs of this annex.

Legal notice

Publisher:
Kraftfahrt-Bundesamt
Postfach 12 01 53
01002 Dresden
Germany

Internet: www.kba.de

Special information and advice:

Phone: +49 461 316-2600
Fax: +49 461 316-2636
E-Mail: benennungsstelle@kba.de

Issued in January 2021
Version: January 2021

Printing: Druckzentrum KBA

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

We score with road safety!