**Manufacturer**[1]

Registration number:

Name:

Audited site:

Date of audit:

Auditor:

## General

This catalogue of requirements contains the requirements of UN-R 155/156 and the type approval procedure of the Kraftfahrt-Bundesamt (Federal Motor Transport Authority) with reference to a cybersecurity and/or software update management system. Its purposes are as follows:

- On receipt of a self-disclosure from the manufacturer, it forms the basis for audit planning;
- With additions from the auditors, as part of the audit report, it forms the basis for the KBA's decision whether or not to issue a certificate of compliance according to Section 6 of UN-R 155 and/or 156.

The requirements apply to all sites, processes and products/services[2] included in the certificate.

In general, a manufacturer must comply with all requirements. Where individual requirements are not applicable, the manufacturer may record this, giving reasons. The auditor is not bound to this statement by the manufacturer but will take it into account when preparing the audit.

The aim of the audit is not to prove 100% security, but to confirm, on the basis of documented requirements and objective evidence from the manufacturer, that:

- There is no significant risk to safety, environment, or health within the scope of UN-R 155/156;
- The requirements of the UN Regulations can be met;
- The manufacturer has implemented the measures documented by it in a satisfactory manner;
- Staff are aware of their responsibility to comply with the requirements.

## Notes for users

Where requirements relate to product tests (by the manufacturer), the relevant requirements according to Section 7.3 of UN-R 155 and/or Section 7.2 of UN-R 156 also apply (cf. note in brackets).

The use of the singular in the requirements (e.g., a process) does not exclude different methods of implementation (e.g. in several processes).

[1] The term 'manufacturer' is here used as a synonym for 'audited organisation' and current and/or future holder of a type approval.

[2] Hereinafter referred to as 'products'.

Compliance with some requirements may be assessed in several audit phases. It is expected that compliance with the requirements is ensured by means of documented appropriate and effective processes and that these processes are regularly assessed on the basis of objective criteria and evidence.

The following abbreviations are used for assessments:

iO - no problems
P - positive finding to be highlighted
V - generally ok, opportunity for improvement
N - minor non-conformity (with number of Report of non-conformity)
H - major non-conformity (with number of Report of non-conformity)
nb - not evaluated
nz - not applicable (reasons required, unless obvious from other information)

Findings P, V, N and H will be explained in the audit report in a summary table under the heading ‘Audit results. Additional explanations on the self-disclosure will be entered by the auditor in italics in the column ‘Manufacturer’s self-disclosure/Auditor’s comments.

The full evaluation is the responsibility of the lead auditor (the person signing the audit report). If the audit is carried out by several auditors, the catalogue of requirements can be split up accordingly. If so, please ensure that on completion of the audit the KBA receives one fully completed copy.

This catalogue of requirements comprises:
- Part A: General requirements for management systems
- Part B: Special requirements for CSMS/SUMS

The manufacturer must ensure that the general requirements (Part A) are applied when implementing the CSMS/SUMS-specific requirements, where appropriate. As an aid, references are made to Part A in Part B, but these are not exhaustive and may not be applicable in every case.

Part B refers to requirements from Part A that must be complied with. To that extent, Part A must not be audited separately.

## List of abbreviations

| | |
|---|---|
| A | Record required[3] |
| CS | Cybersecurity |
| D | Documented process description or the like required |
| E | Assessment |
| KBA | Kraftfahrt-Bundesamt (Federal Motor Transport Authority) |
| MS | Management system |
| SU | Software update |
| TS | Technical Services |

## Other documents having effect

Audit report
Risk assessment checklist
x Test procedures checklists
x Process verification checklists

[3] Records often can only be inspected during monitoring/re-certification.

## Part A – General requirements for management systems

| No. | Additional requirement | E |
|---|---|---|
| 1 | Management takes responsibility | |
| 2 | The elements, processes, requirements etc. of the CSMS/SUMS are not in conflict with other processes, systems, specifications ... of the organisation; interfaces are sufficiently defined | |
| 3 | Decisions made and approvals given in collaboration with largely neutral persons and/or committees, wherever possible | |
| 4 | Objectives are cascaded, consistent, appropriate and measurable;<br>they are communicated appropriately and updated regularly | |
| 5 | Requirements<br>- Derived from objectives and risk analysis<br>- Appropriate<br>- Documented (where needed)<br>- Compliance monitored | |
| 6 | Process<br>- Responsibility/competences<br>- Entry/process/exit/interface to other processes<br>- Performance indicators/suitability criteria (consistent with objectives)<br>- Approval<br>- Skills/knowledge<br>- Work/test equipment<br>- Infrastructure, process environment, time resources etc.<br>- Management of non-compliant results<br>- Monitoring (appropriate, suitable; documentation; analysis)<br>- Documentation | |
| 7 | Other verification of conformity<br>- Organised<br>- Competent<br>- Suitable<br>- Documented | |
| 8 | Marking and traceability | |
| 9 | Knowledge of the organisation (information management)<br>- Collected, recorded, controlled, analysed, used sensibly;<br>- Appropriate communication<br>- Protection against loss, falsification, unauthorised access, cover-up, delay, etc. | |
| 10 | Required competence of management, those carrying out the process, those supervising staff (knowledge, abilities, skills)<br>- Defined<br>- Present<br>- Type and criteria of (first-time and repeated) verification defined<br>- Records of competence assessment | |
| 11 | All relevant persons are aware of their role in achieving the objectives and the consequences of non-conformity with requirements. | |

| No. | Additional requirement | E |
|---|---|---|
| 12 | The organisation has and maintains a continuous improvement process (lessons learned, communication, review of effectiveness) | |
| 13 | Change management (suitable, appropriate, effective) | |
| 14 | Security management (security of information, of buildings, etc.) | |
| 15 | Emergency management | |
| 16 | Escalation management | |
| 17 | Data protection | |

## Part B – Special requirements for CSMS/SUMS

| Requirement | UN-R 155 | UN-R 156 | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| **General requirements for and planning CSMS/SUMS** | | | | | |
| The scope of application of the CSMS/SUMS has been defined; any exclusions are reasoned and justified<br>- Processes<br>- Products<br>- Sites<br>- Environment (e.g., suppliers, outsourcing) | 7.2.2.1 | 7.1.1.1 | D<br>1 | | |
| The CSMS/SUMS covers all phases. The relevant processes (CS/SU in the strict sense and other processes) and interfaces (including to external processes) are sufficiently defined with respect to CS/SU; existing processes and interfaces are adjusted to the required extent | 7.2.2 | 7.1.1 | D<br>2 | | |
| Responsibility of management<br>- Assets to be protected (hardware, software, information) are defined for all phases<br>- Policy and objectives with respect to CS/SU defined (in accordance with the overall objectives of the organisation)<br>- Operational and organisational structure appropriately defined<br>- Monitoring organised, analysed<br>- Responsibilities defined<br>- Understanding/awareness of CS maintained at the required level<br>- Resources made available<br>- Improvement requested<br>- Stability ensured in case of modification etc. | 7.2.2 | 7.1.1 | A<br>1 9 10 11 12 17 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| The exchange of information with the type approval authority and the technical services has been organised and is effective | 6.10 | 6.8 | A<br>9 11 | | |
| **Risk management** | | | | | |
| Assets to be protected have been defined in detail for all phases<br>(including for software before and during update). | 7.2.2.1 | 7.1.3<br>7.2.1.1<br>7.2.1.2 | D<br>1 2 4 5<br>12 | | |
| The risk analysis and the planning of the CSMS/SUMS resulting from this are carried out as a controlled process<br>- Responsibilities<br>- Definition<br>- Monitoring/updating etc. | 7.2.2 | 7.1.1 | D, A<br>3 6 9<br>10 11<br>12 13 | | |
| A comprehensive risk analysis has been carried out<br>- Sources<br>- UN-R 155 Annex 5 and/or UN-R 156<br>- Assets to be protected Vulnerabilities<br>- Attack paths and scenarios<br>- Internal/external factors<br>- Confidentiality, integrity, availability of information<br><br>There are recorded reasons if measures according to UN-R 155 Annex 5 are not implemented<br><br>For details, see the 'risk analysis' checklist | 7.2.2.2<br>7.2.2.3<br>7.2.2.5<br>7.3.2<br>7.3.5 | 7.1.3.1<br>7.1.3.2<br>7.2.1.1<br>7.2.1.2 | A<br>1 3 5 9<br>10 11<br>12 13<br>17 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| For all relevant sites, the risk analysis comprises:<br>- Identification of risks<br>- Probability of occurrence and detection<br>- Consequences/ categorisation<br>- evaluation on the basis of set and adequate criteria<br>- Prioritisation<br>For details, see the 'risk analysis' checklist | 7.2.2.2<br>7.2.2.5<br>7.3.2 | 7.1.3.1<br>7.1.3.2<br>7.2.1.1<br>7.2.1.2 | A<br>1 3 5 9<br>10 11<br>12 13 | | |
| The risk analysis relates to:<br>- Product (vehicle)<br>  - Components and systems<br>  - Their interactions<br>  - Interactions between the vehicle and its individual components/systems with external systems<br>  - Protection against unauthorised (compromised) updates (UN-R 156)<br>- Process<br>  - Processes of the organisation and their interfaces<br>  - Interfaces to external processes<br>  - Processes in the post-production phase<br>  - At all relevant sites<br>- Persons involved<br>- Infrastructure and other external factors to be taken into account by the manufacturer<br>- Software update (incl. back-end and vehicle); R-156 only<br>For details, see the 'risk analysis' checklist | 7.3.3<br>7.2.2.2<br>7.2.2.5<br>7.3.2 | 7.1.3.1<br>7.1.3.2<br>7.2.1.1<br>7.2.1.2 | A<br>1 3 5 9<br>10 11<br>12 13<br>17 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| All critical vulnerabilities are detected, analysed and treated where necessary<br>- Development<br>- Production<br>- Post-production<br>- (Scrapping)<br>- Software update<br>  - Systems and components may be excluded if they demonstrably cannot be updated<br>  - Back-end and vehicle are included | 7.2.2.1<br>7.2.2.2<br>7.2.2.5 | 7.1.3.1<br>7.1.3.2<br>7.1.3.3<br>7.2.1.1<br>7.2.1.2<br>.3 | A<br>5 9–13 | | |
| Effective and appropriate processes have been implemented for attempted or successful attacks in all phases<br>- To be detected,<br>- To be made available to the right bodies in a timely manner and through the appropriate channels,<br>- To be analysed for real and potential direct and indirect impacts;<br>- For measures relating to product, process and prevention to be derived and implemented within a reasonable time-frame (among other things, the risk analysis is updated).<br>- Effective escalation management<br>- Software code and functionality is verified and validated after update; unauthorised (compromised) updates are prevented | 7.2.2.2<br>7.2.2.3 | 7.1.3.1<br>7.1.3.2<br>7.1.3.3<br>7.2.1.1<br>7.2.1.2 | D, A<br>1 2 4–6 8 9–16 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ ***Auditor's comments*** *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| Appropriate measures are derived from the risk analysis When measures have been defined, the risk is re-evaluated and classed as acceptable The efficacy, effectiveness, appropriateness of the measures is assessed over an appropriate period. | 7.2.2.2 | 7 | A<br>2 3 5<br>9-16 | | |
| The interactions between the measures taken as a result of the risk analysis or following incidents are taken into account | 7.2.2.3 | 7 | 2<br>10–16 | | |
| **Requirements for processes** (see checklist for details) | | | | | |
| Product development<br>- Objective<br>- CS/SU requirements (in development contract specifications)<br>- Required inputs<br>- Management of development process<br>- Verification/validation (including, where needed, for different combinations of modules)<br>- Documentation | 7.2.2.2 | 7.1.1 | D, A<br>1–6<br>9–16 | | |
| Construction is based on the risk analysis and the current state of the art (e.g., cryptographic modules) at the time of approval; if not, any divergence is justified | 7.3.8 | 7.1.1 | A<br>5 9–12 | | |
| All relevant processes up to and including the production phase have been sufficiently evaluated and defined with respect to CS/SU risks (incl. production, purchasing, maintenance, service etc.) | 7.2.2 | 7.1.1 | D<br>3 5 6<br>9–16 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| All relevant processes in the post-production phase (e.g., maintenance, accidents, repair, tuning, software update, scrapping etc.)<br>- have been sufficiently assessed and defined with respect to CS/SU risks<br>- The effectiveness of the CS/SU-relevant features integrated into the product is verified/restored (protection, data transfer mechanisms etc.)<br>- Market surveillance tasks (e.g., read-out of information on potential attacks)<br><br>During servicing/repairs, the risk level is not increased; available information sources are used (e.g., memory read-out); confidentiality, integrity and availability are maintained during servicing and transfer of information | 7.2.2.2<br>7.2.2.4<br>7.2.2.5 | 7.1.1 | D<br>3 5 6<br>9–16 | | |
| Security is ensured in all relevant processes (production, warehousing, maintenance, service etc.)<br>Risks are managed in case of modifications to processes or the process landscape. | 7.2.2.2 | - | 1 6 14 | | |
| There is a process for verifying (and ensuring) that over-the-air updates conducted during driving will not impact safety. | - | 7.1.4.1 | D<br>6 9.12<br>13 15<br>16 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| There are process-related arrangements to ensure that an over-the-air update can only proceed when, where necessary, personnel skilled to perform the update is in control of the process. | - | 7.1.4.2 | A D 6 9 12 13 15 16 | | |
| Required processes (R-156)<br>- Information management<br>- Software identification and validation of its integrity (including relevant hardware)<br>- RXSWIN management (including affected software and hardware)<br>- Verification of the software installed in respect of the RXSWIN (storage of frozen state of the software for 10 years after production is discontinued)<br>- Evidence of the updated systems' independence from other systems<br>- Identification of target vehicles for a software update<br>- Confirmation of the compatibility of the update with the target vehicle's (specific software) configuration before the update starts<br>- Assessment whether the update will affect any system type approvals (including identification parameters) (documentation of assessment process)<br>- Assessment whether the update will alter the vehicle compared to when it was originally approved (documentation of assessment process) | - | 7.1.1.1<br>7.1.1.2<br>7.1.1.3<br>7.1.1.4<br>7.1.1.5<br>7.1.1.6<br>7.1.1.7<br>7.1.1.8<br>7.1.1.9 | A D 2 3 6 9 11–13 15 16 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| - Assessment whether the update will affect the safe operation and functionality of the vehicle compared to when it was originally approved (documentation of assessment process)<br>- Driver is informed of the update<br>- Information on software modifications and affected vehicles can be made available to authorised external parties | | 7.1.1.10<br>7.1.1.11<br>7.1.1.12 | A D 2 3 6 9 11–13 15 16 | | |
| Update process<br>- Process description and evidence of compliance with the processes described<br>- Description of the configuration of any relevant type-approved system before/after update (including unique identification of hardware/software/ parameters)<br>- Register of information for every RXSWIN with respect to software before/after the update (including all relevant vehicle/system parameters)<br>- List of all target vehicles and confirmation of their compatibility with the update<br>- Documentation of the update (see 7.1.2.5 a–i) | | 7.1.2<br>7.1.2.1<br>7.1.2.2<br>7.1.2.3<br>7.1.2.4<br>7.1.2.5 | | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| **Other requirements according to UN-R 156** | | | | | |
| RXSWIN<br>- Uniquely identifiable<br>- Updated if the update concerns type-approval-relevant software<br>- Interface easily readable, at least by the OBD port (if the RXSWIN is not held on the vehicle, at least the software version is to be declared to the approval authority)<br>- Protected against manipulation (measures to be confidentially provided to the Approval Authority) | - | 7.2.1.2 | A D<br>5–16 | | |
| Over-the-air update requirements of the vehicle<br>- In case of a failed update, the previous state can be restored or the vehicle is placed into a safe state<br>- Update only possible if the vehicle has enough power to complete the update and to perform recovery measures if necessary (see above) | - | 7.2.2.1 | A D<br>5–16 | | |

| Requirement | UN-R 155 | UN-R 156 | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| Over-the-air update<br>Additional requirements<br>- In case of safety-relevant updates, the vehicle is placed into a safe state by technical measures<br>- The vehicle user is informed about the update according to 7.2.2.2 before the update is executed<br>- If the update is not possible during driving, the vehicle cannot be moved during the execution of the update and the driver is not able to use any functionality of the vehicle that would affect its safety<br>- The vehicle user is informed of the success or failure of the update<br>- The vehicle user is informed of any changes and any updates to the user manual, if applicable<br>- The vehicle shall ensure that any preconditions are met before the software update is executed | - | 7.2.2.1<br>7.2.2.2 | A D<br>5–16 | | |
| **Processes, products, services provided by external parties** | | | | | |
| Assessment, selection, performance monitoring and re-assessment of external sources/outsourced processes<br>- Defined (criteria, procedures, responsibilities etc.)<br>- Appropriate (according to risk analysis)<br>- Effective | 7.2.2.5<br>7.3.2 | | D A<br>5 6 8-<br>12 14 | | |
| Clear and legally binding description of the service to be rendered and the security measures to be complied with; Appropriate inspection of the product/service supplied | 7.2.2.5<br>7.3.2 | | A<br>5 7 8<br>10–12 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ ***Auditor's comments*** *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| Protection of security-relevant information is sufficiently organised and implemented (with the external supplier; when exchanging information) | 7.3.2 | | 1 9–12 14–16 | | |
| **Monitoring and measuring** (see checklists for details) | | | | | |
| Where appropriate, inspections are planned and carried out in the<br>- Production phase<br>- Post-production phase/servicing | 7.3.5 | 7.1<br>7.2 | D, A<br>6 7 9–13 | | |
| Testing instructions exist where necessary<br>- Parameters to be tested<br>- Test procedures<br>- Test equipment<br>- Acceptance criteria<br>These are understandable to the relevant user. | 7.2.2.2<br>7.3.6 | 7.1<br>7.2 | D<br>6 7 9–12 16 | | |
| Test results are analysed and, where necessary, corrections/corrective measures are established and initiated. | 7.2.2.2<br>7.3.4 | 7.1.3.1<br>7.1.3.2<br>7.1.3.3<br>7.2.1.1<br>7.2.1.2.3 | A<br>1 9–13 16 | | |
| There is an appropriate programme for internal CSMS/SUMS audits, which is implemented and includes all relevant areas and sites (including servicing); priorities are set. | 7.2.2. | 7.1.1 | D, A<br>1 5 6 9–12 | | |
| The supplier's compliance with the requirements for ensuring CS/SU is monitored. | 7.2.2.2<br>7.2.2.5<br>7.3.5 | 7.1.3.1<br>7.1.3.2<br>7.1.3.3<br>7.2.1.1<br>7.2.1.2 | A<br>7–13 16 | | |
| CoP is ensured in accordance with the 1958 agreement. Results are recorded and stored for the period agreed with the Approval Authority. | 9 | 9 | A, D<br>7, 11–13 | | |

| Requirement | UN-R | | General requirement | Manufacturer's self-disclosure/ *Auditor's comments* *(in italics)* (Reference may be made to MS documents, stating the relevant section) | E |
|---|---|---|---|---|---|
| | 155 | 156 | | | |
| Market surveillance is organised<br>- Sources (vehicle, user, service operations etc.)<br>- Responsibilities<br>- Reporting obligations, reporting channels<br>- Protection of information<br>- Analysis; if applicable, measures and adjustments to risk analysis | 7.2.2.2<br>7.2.2.5 | - | A, D<br>1 3–6<br>9–16 | | |
| Assessment reports and opportunities for improvement from the last audit have been sufficiently processed. Corrective measures are effective. | 7.2.2 | 7.1.1 | A<br>1<br>10–13 | | |
| Feststellungsprotokolle und Verbesserungspotenzial der letzten Auditierung wurden ausreichend bearbeitet. Korrekturmaßnahmen sind effektiv. | 7.2.2 | 7.1.1 | A<br>1<br>10-13 | | |
| **Other**[4] | | | | | |
| | | | | | |

[4] will be filled only by the KBA