Risk Analysis Checklist
according to UN-R 155, Annex 5

KBA

Reg. no.   No.

Date of assessment   Date

Assessed by   Name

	Annex 5 No.	ok	nok	na/ne/comment
Back-end servers related to vehicles in the field				
− Attack on the vehicle	1	☐	☐	
− Unauthorised access to data	1	☐	☐	
− Attack on back-end server	2	☐	☐	
− Attack on communication channel between back-end server and vehicle	2	☐	☐	
− Loss of vehicle-related data (identification, control, ...)	3	☐	☐	
− Falsification of vehicle-related data (identification, control, ...)	3	☐	☐	
Communication with the vehicle				
− Spoofing of data for the vehicle	4	☐	☐	
− Spoofing, erasure, other modification of vehicle-held data	5	☐	☐	
− Manipulation by unreliable or untrusted sources	6	☐	☐	
− Manipulation by interception of data	7	☐	☐	
− Manipulation by accessing sensitive data	7	☐	☐	
− Manipulation of vehicle functions	8	☐	☐	
− Manipulation by access by unprivileged user	9	☐	☐	
− Manipulation by malicious software (malware)	10	☐	☐	
− Manipulation by malicious messages received	11	☐	☐	
− Manipulation by malicious in-vehicle messages	11	☐	☐	
Update of the vehicle				
− Compromise of over-the-air software update procedures	12	☐	☐	
− Compromise of local software update procedures	12	☐	☐	
− Compromise by manipulated update software	12	☐	☐	
− Compromise by preventing critical software updates	13	☐	☐	
Access by unintentional actions				
− Access by unintentionally loading malware	15	☐	☐	
− Access by no following security procedures	15	☐	☐	
External connectivity and connections				
− Manipulation of functions designed to remotely operate the vehicle	16	☐	☐	
− Manipulation of vehicle telematics	16	☐	☐	
− Manipulation by wireless systems	16	☐	☐	
− Access by manipulated applications	17	☐	☐	
− Access via external interfaces (e.g., USB, OBD)	18	☐	☐	
Vehicle data/code				
− Access to personal data and software	19	☐	☐	
− Manipulation of personal or vehicle data (identity theft, falsifying vehicle parameters)	20	☐	☐	
− Erasure of personal or vehicle data	21	☐	☐	
− Introduction of malicious software (new software)	22	☐	☐	
− Introduction of manipulative malicious software (overwriting existing software)	23	☐	☐	
− Disruption of operations	24	☐	☐	
− Manipulation of vehicle parameters	25	☐	☐	
Potential vulnerabilities				
− Unsuitable encryption keys	26	☐	☐	
− Use of deprecated cryptographic algorithms	26	☐	☐	
− Hardware or software engineered to enable an attack	27	☐	☐	

	Annex 5 No.	ok	nok	na/ne/comment
− Software bugs as a result of inadequate testing or poor programming	28	☐	☐	
− Access via internet ports	29	☐	☐	
− Access via other network interfaces	29	☐	☐	
− Unintended transfer of data (e.g., sale of vehicle, change of hired vehicle)	31	☐	☐	
− Manipulation by additional hardware	32	☐	☐	
− Manipulation by hardware replacement	32	☐	☐	

Documents assessed:

Kraftfahrt-Bundesamt • Section 431 • Phone +49 461 316-2600 • Fax: +49 461 316-2636
E-Mail: benennungsstelle@kba.de • Internet: www.kba.de

Revision 1.1, updated 01/2021   Page 2 of 2