Submitted by the IWG on VMAD

Informal document **GRVA-05-18**
5th GRVA, 10-14 February 2020
Agenda item 4(a)

Draft Annex 4 on audit/CEL to the new UN Regulation on Automated Lane Keeping Systems (ALKS)

I Justification

As agreed at the last GRVA, this text was drafted as an Annex to the draft new UN Regulation on Automated Lane Keeping Systems (ALKS) to address the "audit/assessment/simulation/in use reporting" pillar when applied to Automated Lane Keeping Systems. The text is based on the structure of Annex 6 to UN Regulation No. 79 (steering equipment) on Complexed Electronic Systems (CEL) as lastly amended by GRVA in September 2019 (so called CEL annex – step 2).

Main changes to lastly amended CEL Annex are the following:

- Tailor it to Automated driving functions (e.g. ALKS but not only), not a generic annex for any electronic/driver assistant systems.

- Cover operational safety and not only functional safety.

- Clarify the safety target (free from unreasonable risk for humans)

- Clarify that the Type Approval Authority is main responsible authority (or the technical service on their behalf) for the audit, as it is already the case for the rest of the type approval system.

- Clarify that, notwithstanding the audit/assessment made by the type-approval authority, the manufacturer is the responsible for safety with regard to the requirements of this Regulation.

- Specify documentation layout and transparency of information across authorities

- Specify the necessary competences of the auditor.

- Specify the content of the manufacturer safety management system (safety culture) including lifetime/lifecycle aspects

- Provides basic requirements for the use virtual testing/ simulation tools

This text below is in line with other papers discussed in VMAD, namely the concept paper and the proposed *building blocks* for audit/assessment reporting pillar. However, compared to the *building blocks*, some elements have not been included at this stage due to the time constraints:

- Independent formal proof for safety aspects of supplied components (e.g. "units" or "electronic control systems") which can form part of any system

- Specifying at which stages of product development the different steps of the audit/assessment shall take place (e.g. review of the safety concept before production shall take place)

- Renewal of the assessment/audit. Monitoring by the authority.

- Rating of audit (major/minor failure, etc).

The text below is also in line with the concept papers for scenarios and physical testing discussed in VMAD and the core text of the ALKS regulation/testing annex as discussed in the ACSF informal working group.

The document is almost final. However a number of issues may deserve a discussion in GRVA, namely:

- Scope and limits of the inspection done by authorities and responsibility of manufacturers in terms of safety.

- The level of requirements on manufacturers concerning the support of their vehicles during their lifetime (similar discussion for cybersecurity).

- Level of information to be shared amongst authorities and what shall kept at manufacturer level.

-Whether some requirements fit better in this annex of in other parts of the ALKS regulation (e.g. information document/information data).

II Proposal

Annex 4

Special requirements to be applied to the functional and operational safety aspects of automated driving systems

1. General

This annex is intended to ensure that an acceptable thorough consideration of functional and operational safety for the automated driving system has been performed by the manufacturer during the design and development processes and will continue to be done throughout the vehicle type lifecycle (design, development, production, field operation, decommissioning).

It covers the documentation which must be disclosed by the manufacturer to the type-approval authority or the technical Service acting on its behalf (hereafter referred as type-approval authority), for type approval purposes.

This documentation shall demonstrate that "The System" meets the performance requirements specified in this UN Regulation, that it is designed/developed to operate in such a way that the automated driving system is free of unreasonable safety risks to the driver, passengers and other road users.

The type approval authority granting the approval shall verify through targeted spot checks and tests that the argumentation provided by the documentation is strong enough and that the design/processes described in documentation are actually implemented by the manufacturer.

While based on the provided documentation, evidence and process audits/product assessments carried out to the satisfaction of the type approval authority concerning this Regulation, the residual level of risk of the assessed automated driving system is deemed to be acceptable for the entry into service of the vehicle type, the overall vehicle safety during the vehicle lifetime in accordance with the requirements of this regulation remains the responsibility of the manufacturer requesting the type-approval.

2. Definitions

For the purposes of this annex,

2.1. "*The System*" means a "*Higher-Level Electronic Control" system and its electronic control system(s)* that provide the automated driving function(s) regulated by this Regulation. This also includes any transmission links to or from other systems that are outside the scope of this Regulation, that acts on the function to which this Regulation applies.

2.2. "*Safety Concept*" is a description of the measures designed into the system, for example within the electronic units, so that the vehicle operates in such a way that it is free of unreasonable safety risks to the driver, passengers and other road users under faults and non-fault conditions. The possibility of a fall-back to partial operation or even to a back-up system for vital vehicle functions shall be a part of the safety concept.

2.3. "*Electronic control system*" means a combination of units, designed to co-operate in the production of the stated automated driving function by electronic data processing. Such systems, commonly controlled by software, are built from discrete functional components such as sensors, electronic control units and actuators and connected by transmission links. They may include mechanical, electro-pneumatic or electro-hydraulic elements.

2.5. "*Higher-Level Electronic Control*" systems are those which employ processing and/or sensing provisions to realize the dynamic driving task.

2.6. "*Units*" are the smallest divisions of system components which will be considered in this annex, since these combinations of components will be treated as single entities for purposes of identification, analysis or replacement.

2.7. "*Transmission links*" are the means used for inter-connecting distributed units for the purpose of conveying signals, operating data or an energy supply. This equipment is generally electrical but may, in some part, be mechanical, pneumatic or hydraulic.

2.8. "*Range of control*" refers to an output variable and defines the range over which the system is likely to exercise control.

2.9. "*Boundary of functional operation*" defines the boundaries of the external physical limits within which the system is able to perform the dynamic driving tasks.

2.9.1. "*Operational design domain (ODD)*" of the automated driving system defines the specific operating conditions (e.g. environmental, geographic, time-of-day, traffic, infrastructure, speed range, weather and other conditions) within the boundaries fixed by this regulation under which the automated driving system is designed to operate without any intervention by the driver.

2.10. "*Automated Driving Function*" means a function of "The System" that is capable of performing the dynamic driving tasks of the vehicle.

2.11. "*Control strategy*" means a strategy to ensure robust and safe operation of the function(s) of "The System" in response to a specific set of ambient and/or operating conditions (such as road surface condition, traffic intensity and other road users, adverse weather conditions, etc.). This may include the automatic deactivation of a function or temporary performance restrictions (e.g. a reduction in the maximum operating speed, etc.).

2.12. "*Functional safety":* absence of unreasonable risks under the occurrence of hazards caused by a malfunctioning behaviour of electric/electronic systems (safety hazards resulting from system faults).

2.13. *"Fault":* abnormal condition that can cause an element (system, component, software) or an item (system or combination of systems that implement a function of a vehicles) to fail.

2.14. *"Failure"* means the termination of an intended behaviour of an element or an item.

2.13. *"Operational safety"* means the absence of unreasonable risk under the occurrence of hazards resulting from functional insufficiencies of the intended functionality (e.g. false/missed detection), operational disturbances (e.g. environmental conditions like fog, rain, shadows, sunlight)) or by reasonably foreseeable misuse by persons (safety hazards — without system faults).

3. Documentation

3.1. Requirements

The manufacturer shall provide a documentation package which gives access to the basic design of "The System" and the means by which it is linked to other vehicle systems or by which it directly controls output variables.

The function(s) of "The System", including the control strategies, and the safety concept, as laid down by the manufacturer, shall be explained.

Documentation shall be brief, yet provide evidence that the design and development has had the benefit of expertise from all the system fields which are involved.

For periodic technical inspections, the documentation shall describe how the current operational status of "The System" can be checked.

The Type-approval authority shall assess the documentation package to show that "The System" within the declared ODD:

(a) Is designed and was developed to operate in such a way that it is free from unreasonable risks for the driver, passengers and other road users;

(b) Respects, under the performance requirements specified elsewhere in this UN Regulation;

(c) Was developed according to the development process/method declared by the manufacturer and that this includes at least the steps listed in paragraph 3.4.4.

(d) Is designed to recognize its ODD limits

(e) Does not operate outside of the declared ODD and any attempt to activate the System outside of the ODD will not lead to activation

3.1.1. Documentation shall be made available in 3 parts:

(a) Application for type approval: The information document which is submitted to the type approval authority at the time of type approval application shall contain brief information on the items listed in Appendix 2. It will become part of the approval.

(b) The formal documentation package for the approval, containing the material listed in this section 3. (with the exception of that

of paragraph 3.4.4.) which shall be supplied to the Type Approval Authority for the purpose of conducting the product assessment / process audit. This documentation package shall be used by the Type Approval Authority as the basic reference for the verification process set out in paragraph 4. of this annex. The Type Approval Authority shall ensure that this documentation package remains available for a period determined of at least 10 years counted from the time when production of the vehicle type is definitely discontinued.

(c) Additional confidential material and analysis data (intellectual property) of paragraph 3.4.4. which shall be retained by the manufacturer, but made open for inspection (e.g. on-site in the engineering facilities of the manufacturer) at the time of the product assessment / process audit. The manufacturer shall ensure that this material and analysis data remains available for a period of 10 years counted from the time when production of the vehicle is definitely discontinued.

3.2. Description of the functions of "The System" including control strategies

A description shall be provided which gives a simple explanation of all the functions including control strategies of "The System" and the methods employed to perform the dynamic driving tasks within the boundaries under which the automated driving system is designed to operate, including a statement of the mechanism(s) by which control is exercised. The manufacturer shall describe the interactions expected between the system with the driver, vehicle occupants and other road users.

Any enabled or disabled automated driving functions providing when the hardware and software are present in the vehicle at the time of production, shall be declared and are subject to the requirements of this annex, prior to their use in the vehicle. The manufacturer shall also document the data processing in case of continuous learning implemented.

3.2.1. A list of all input and sensed variables shall be provided and the working range of these defined, along with a description of how each variable affects system behaviour."

3.2.2. A list of all output variables which are controlled by "The System" shall be provided and an indication given, in each case, of whether the control is direct or via another vehicle system. The range of control (paragraph 2.7.) exercised on each such variable shall be defined.

3.2.3. Limits defining the boundaries of functional operation including ODD-limits shall be stated where appropriate to system performance.

3.2.4 Interaction concept with the driver when ODD limits are reached shall be explained including an overview of types of situations in which the system will generate a transition demand to the driver.

3.3. System layout and schematics

3.3.1. Inventory of components.

A list shall be provided, collating all the units of “The System” and mentioning the other vehicle systems which are needed to achieve the control function in question.

An outline schematic showing these units in combination, shall be provided with both the equipment distribution and the interconnections made clear.

This outline shall include:

- Perception and objects detection including mapping and positioning

- Characterization of Decision-making

- Remote supervision and remote monitoring by a remote supervision (if applicable).

- Perception and objects detection including mapping and positioning

3.3.2. Functions of the units

The function of each unit of “The System” shall be outlined and the signals linking it with other units or with other vehicle systems shall be shown. This may be provided by a labelled block diagram or other schematic, or by a description aided by such a diagram.

3.3.3. Interconnections within “The System” shall be shown by a circuit diagram for the electric transmission links, by a piping diagram for pneumatic or hydraulic transmission equipment and by a simplified diagrammatic layout for mechanical linkages. The transmission links both to and from other systems shall also be shown.

3.3.4. There shall be a clear correspondence between transmission links and the signals carried between Units. Priorities of signals on multiplexed data paths shall be stated wherever priority may be an issue affecting performance or safety.”

3.3.5. Identification of units

Each unit shall be clearly and unambiguously identifiable (e.g. by marking for hardware, and by marking or software output for software content) to provide corresponding hardware and documentation association.

Where functions are combined within a single unit or indeed within a single computer, but shown in multiple blocks in the block diagram for clarity and ease of explanation, only a single hardware identification marking shall be used. The manufacturer shall, by the use of this identification, affirm that the equipment supplied conforms to the corresponding document.

3.3.5.1. The identification defines the hardware and software version and, where the latter changes such as to alter the function of the Unit as far as this Regulation is concerned, this identification shall also be changed.

3.4. Safety concept of the manufacturer

3.4.1. The Manufacturer shall provide a statement which affirms that the “The System” is free from unreasonable risks for the driver, passengers and other road users.

3.4.2. In respect of software employed in "The System", the outline architecture shall be explained and the design methods and tools used shall be identified (see 3.5.1). The manufacturer shall show evidence of the means by which they determined the realization of the system logic, during the design and development process.

3.4.3. The Manufacturer shall provide the Type Approval Authority with an explanation of the design provisions built into "The System" so as to

ensure functional and operational safety. Possible design provisions in "The System" are for example:

(a) Fall-back to operation using a partial system.

(b) Redundancy with a separate system.

(c) Removal of the automated driving function(s).

fault3.4.3.1. If the chosen provision selects a partial performance mode of operation under certain fault conditions, then these conditions shall be stated and the resulting limits of effectiveness defined.

3.4.3.2. If the chosen provision selects a second (back-up) means to realise the performance of the dynamic driving tasks, the principles of the change-over mechanism, the logic and level of redundancy and any built in back-up checking features shall be explained and the resulting limits of back-up effectiveness defined.

3.4.3.3. If the chosen provision selects the removal of the Higher Level Function, this shall be done in compliance with the relevant provisions of this regulation (e.g. on minimum risk manoeuver and transition demand). All the corresponding output control signals associated with this function shall be inhibited, and in such a manner as to limit the transition disturbance.

3.4.4. The documentation shall be supported, by an analysis which shows, in overall terms, how the system will behave to mitigate or avoid hazards which can have a bearing on the safety of the driver, passengers and other road users.

The chosen analytical approach(es) shall be established and maintained by the Manufacturer and shall be made open for inspection by the Type-approval authority at the time of the type approval.

The Type-approval authority shall perform an assessment of the application of the analytical approach(es):

(a) Inspection of the safety approach at the concept (vehicle) level.

This approach shall be based on a Hazard / Risk analysis appropriate to system safety.

(b) Inspection of the safety approach at the system level including a top down (from possible hazard to design) and bottom up approach (from design to possible hazards). The safety approach may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) and a system-theoretic process analysis (STPA) or any similar process appropriate to system functional and operational safety.

(c) Inspection of the validation/verification plans and results including appropriate acceptance criteria. This shall include validation testing appropriate for validation, for example, Hardware in the Loop (HIL) testing, vehicle on-road operational testing, or any other testing appropriate for validation/verification.

The inspection shall confirm that each of the following items is covered where applicable under (a)-(c):

(i) Interactions with other vehicle systems (e.g. braking, steering);

(ii) Failures of the automated driving system and system risk mitigation reactions;

(iii) Situations within the ODD when a system may create unreasonable safety risks for the driver, passengers and other road users due to operational disturbances (e.g. lack of or wrong comprehension of the vehicle environment, inadequate control, challenging scenarios)

(iv) Identification of the relevant scenarios within the ODD and management method used to select scenarios and validation tool chosen

(v) Decision making resulting in performance of the dynamic driving tasks (including e.g. emergency manoeuvres) and interaction with other road users and in compliance with traffic rules

(vi) Reasonably foreseeable misuse by the driver driver (including e.g. driver availability recognition system and an explanation on how the availability criteria were established) and intentional tampering of the system.

(viii) Cyber-attacks having an impact on the safety of the vehicle (can be done through the analysis done under the cyber regulation).

The assessment by the approval authority shall consist of spot checks of selected hazards (or cyber threats) to establish that argumentation supporting the safety concept is understandable and logical and implemented in the different functions of the systems. The assessment shall also check that validation plans are robust enough to demonstrate safety and have been completed.

It shall demonstrate that the vehicle is free from unreasonable risks for the driver; vehicle occupants and other road users in the operational design domain:

- The safety demonstration shall include a quantitative pre-validation target (e.g., using validation acceptance criteria), documented by the manufacturer, demonstrating that the introduction of the ADS will overall not increase the level of risk for the driver, passengers and other road users compared to a manually driven vehicles; and

- A qualitative approach showing that the overall level of risks have been minimized during development to a acceptable level for the driver, vehicle occupants and other road users.

The Type Approval Authority shall perform or shall require to perform tests as specified in paragraph 4. to verify the safety concept.

3.4.4.1. This documentation shall itemize the parameters being monitored and shall set out, for each failure condition of the type defined in paragraph 3.4.4. of this annex, the warning signal to be given to the driver/passengers/other road users and/or to service/technical inspection personnel.

3.4.4.2. This documentation shall also describe the measures in place to ensure the "The System" is free from unreasonable risks for the driver, passengers and other road users when the performance of "The System" is affected by environmental conditions e.g. climatic, temperature, dust ingress, water ingress, ice packing.

3.5. Safety management system (Process Audit)

3.5.1 In respect of software and hardware employed in “The System”, the manufacturer shall demonstrate to the type approval authority in terms

of a safety management system that effective processes/methodologies/tools are in place, up to date and being followed within the organization to manage the safety and continued compliance throughout the product lifecycle (design, development, production, operation including respect of traffic rules, decommissioning).

3.5.2. The design/development process shall be established including safety management system, requirements management, requirements' implementation, testing, failure tracking, remedy and release

3.5.3. The manufacturer shall institute and maintain effective communication channels between functional/operational safety, cybersecurity and any other relevant disciplines related to the achievement of vehicle safety.

3.5.4. The manufacturer shall have processes to monitor safety-relevant incident/accidents caused by the engaged automated driving systems and a process to manage potential safety-relevant gaps post-registration (closed loop of field monitoring). They shall [have a process to] report critical incidents (e.g. collision with another road users) to the type-approval authorities when they occur.

3.5.5. The manufacturer shall demonstrate that periodic independent internal process audits are carried out to ensure that the processes established in accordance with paragraphs 3.5.1 to 3.5.4. are implemented consistently

3.5.6. Manufacturers shall put in place suitable arrangements (e.g. contractual arrangements, clear interfaces, quality management system) with suppliers to ensure that the supplier safety management system comply with the requirements of paragraph 3.5.1. to 3.5.5.

4. Verification and tests

4.1. The functional operation of "The System", as laid out in the documents required in paragraph 3., shall be tested as follows:

4.1.1. Verification of the function of "The System"

The Type approval authority shall verify "The System" under non-failure conditions by testing on a track a number of selected functions from those described by the manufacturer in paragraph 3.2. above, and by checking the overall behaviour of the system in real driving conditions including the compliance with traffic rules.

These tests shall include scenarios whereby the system is overridden.

4.1.1.1. The verification results shall correspond with the description, including the control strategies, provided by the manufacturer in paragraph 3.2. and shall comply with the requirements of this regulation.

4.1.2. Verification of the safety concept of paragraph 3.4.

The reaction of "The System" shall be checked under the influence of a faults in any individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal failure within the unit. The Type approval authority shall conduct this check for at least one individual unit, but shall not check the reaction of "The System" to multiple simultaneous failures of individual units.

The Type Approval Authority shall verify that these tests include aspects that may have an impact on vehicle controllability and user information (HMI aspects e.g. transition scenarios).

4.1.2.1 The Type Approval Authorities shall also check a number of scenarios that are critical for the object event detection and characterization of the decision-making and HMI functions of the system within the ODD concerned (e.g. object difficult to detect or when the system reaches the boundaries) as defined in the regulation.

4.1.2.2. The verification results shall correspond with the documented summary of the hazard analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate and in compliance with the requirements of this regulation.

4.2. Simulation tool and mathematical models for verification of the safety concept may be used in accordance with Schedule 8 of Revision 3 of the 1958 Agreement, in particular for scenarios that are difficult on a test track or in real driving conditions. Manufacturers shall demonstrate the scope of the simulation tool, its validity for the scenario concerned as well as the validation performed for the simulation tool chain (correlation of the outcome with physical tests).

5. Reporting

Reporting of the assessment shall be performed in such a manner that allows traceability, e.g. versions of documents inspected are coded and listed in the records of the Technical Service.

An example of a possible layout for the assessment form from the Technical Service to the Type Approval Authority is given in Appendix 1 to this Annex.

6. Communication to the other Type Approval Authorities (See Appendix 3) - it could also be annexed to the Communication form)

- Description of the ODD and the high level functional architecture focusing on the functions available to the driver, passengers and other road users.

- Test results during the verification process by the type approval authorities.

7. Competence of the auditors/assessors

The assessments under this Annex may only be conducted by auditors/assessors with the technical and administrative knowledge necessary for such purposes. They shall in particular be qualified as auditor/assessor for functional and operational safety for ISO 26262-2018: on functional safety for road vehicles, and ISO PAS ISO/PAS 21448: Safety of the Intended Functionality of road vehicles; and being able to make the link with cybersecurity (ISO/SAE DIS 21434).

Annex 4 - Appendix 1

Model assessment form for automated driving systems

Test report No: .....

1. Identification

1.1. Make: .....

1.2. System Type: .....

1.3. Means of system identification on the vehicle: .....

1.4. Location of that marking: .....

1.5. Manufacturer's name and address: .....

1.6. If applicable, name and address of manufacturer's representative: .....

1.7. Manufacturer's formal documentation package:

Documentation reference No: .....
Date of original issue: .....
Date of latest update: .....

2. Test vehicle(s)/system(s) description

2.1. General description: .....

2.2. Description of all the control functions of "The System", and methods of operation: .....

2.3. Description of the components and diagrams of the interconnections within "The System":

2.4. General description: .....

2.5. Description of all the control functions of "The System", and methods of operation: .....

2.6. Description of the components and diagrams of the interconnections within "The System": .....

3. Manufacturer's safety concept

3.1. Description of signal flow and operating data and their priorities: .....

3.2. Manufacturer's declaration:

The manufacturer(s) ..... *affirm(s) that the "The System"* is free from unreasonable risks for the driver, passengers and other road users .

3.3. Software outline architecture and the design methods and tools used: .....

3.4. Explanation of design provisions built into "The System" : .....

3.5. Documented analyses of the behaviour of "The System" under individual hazard or fault conditions: .....

3.6. Description of the measures in place for environmental conditions: .....

3.7. Provisions for the periodic technical inspection of "The System": .....

3.8. Results of "The System" verification test, as per para. 4.1.1. of Annex X to UN Regulation No. XX: .....

3.9. Results of safety concept verification test, as per para. 4.1.2. of Annex X to UN Regulation No. XX: .....

3.10. Date of test(s):.....

3.11. This test(s) has been carried out and the results reported in accordance with ….. to UN Regulation No. XX as last amended by the ..... series of amendments.

Technical Service carrying out the test
Signed: ..... Date: .....

3.12. Comments: .....

Annex 4 - Appendix 2: Information document form for Automated Driving System to be provided by the manufacturer for the approval

1. **System description Automated Lane Keeping System**
   - 1.1. Operational Design Domain (Speed, road type, country, Environment, Road conditions,etc)/ Boundary conditions/ Main conditions for Minimum risk manoeuvres and transition demands
   - 1.2. Basic Performance (e.g. OEDR …)
   - 1.4. The means to activate, override or deactivate the system.
   - 1.5. Expected driver's tasks within the ODD and when going out of the ODD.

2. **Description of the functions of "The System" including control strategies**
   - 2.1. Main automated Driving Functions (functional architecture, environmental perception).
     - 2.1.1. Vehicle-internal
     - 2.1.2. Vehicle-external (e.g. backend)
3. **Overview major components (units) of "The System"**
   - 3.1. Control Units
   - 3.2. Sensors
   - 3.3. Maps/Positioning

4. **System layout and schematics**
   - 4.1. Schematic system layout including sensors for the environmental perception
   - 4.2. List and schematic overview of interconnections
   - 4.3. List of major input variables
   - 4.4. List of major output variables
   - 4.5. Signal flow and priorities
5. **Specifications**
   - 5.1. Means to check the correct operational status of the system
   - 5.2. Means implemented to protect against simple unauthorized activation/operation and interventions into the system
   - 5.3. Operational Design Domain (System boundaries)
6. **Safety Concept**
   - 6.1. Safe Operation – Vehicle Manufacturer Statement
   - 6.2. Outline software architecture
   - 6.3. Means by which the realization of the system logic is determined
   - 6.4. Explanation of the design provisions built into "The System" so as to generate safe operation and interaction with other road users under fault conditions, under operational disturbances and the occurrence of planned/unplanned conditions that would exceed the ODD.
   - 6.5. Failure handling, fall-back level strategy including risk mitigation strategy (minimum risk manoeuvre)
   - 6.6. Analysis on system behaviour on occurrence of faults and operational disturbances
   - 6.7. Driver, vehicle occupants and other road users interaction including warning signals and transition demands to be given to driver.
   - 6.8. Validation by the manufacturer of the performance requirements specified elsewhere in the regulation including the OEDR, the HMI, the respect of traffic rules and the conclusion that that the system is designed in such a way that it is free from unreasonable risks for the driver, vehicle occupants and other road users.
7. **Verification and test by the authorities**
   - 7.1. Verification of the basic function of "The System"
   - 7.2. Examples for checking the system reaction under the influence of a failure or a operational disturbance, emergency conditions and boundary conditions
8. **EDR/ Data Storage System**
   - 8.1. Type of Data stored
   - 8.2. Storage location
   - 8.3. Storage duration
   - 8.4. Means to ensure data security and data protection
   - 8.5. Access to the data

9. Cyber security (cross reference to the cyber regulation is possible)

9.1. Description of the cyber security and software update management scheme
9.2. Description of the different risks and measures put in place to mitigate these risks.
9.3. Description of the update procedure.

10. Information provisions to users

10.1. Model of the information provided to users.
10.2. Extract of the relevant part of the owner`s manual