Study on the assessment and certification of automated vehicles

Final Report

[Written by: Mervyn Edwards, Matthias Seidl, Michelle Tress, Ashley Pressley and Saket Mohan: TRL]
[*December – 2016*]

TRL

EUROPEAN COMMISSION

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
Directorate C — Industrial Transformation and Advanced Value Chains

Unit C.4 — Automotive and mobility Industries

Contact: Antony Lagrange

E-mail: Antony.LAGRANGE@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Study on the assessment and certification of automated vehicles

Final Report

Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs
December *2016*6

Europe Direct is a service to help you find answers to your questions about the European Union.

Freephone number (*):

00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Luxembourg: Publications Office of the European Union, 2014

ISBN 978-92-79-65253-0
doi: 10.2873/548794

Printed in Belgium

Table of contents

Executive summary

The objective of the United Nations (UN) World Forum for Harmonisation of Vehicle Regulations (WP.29) is to initiate and pursue actions aimed at the development or worldwide harmonisation of technical regulations for vehicles. WP.29 has a subsidiary body, the Working Party on Brakes and Running Gear (GRRF), dedicated to the preparation of regulatory proposals on active safety, braking and running matters. As part of this technical area there is an Informal Working Group (IWG) which is considering Automatically Commanded Steering Functions (ACSFs). Initiated in February, 2015; the Terms of Reference for this group (Informal Document ACSF-01-02) begin with the requirement that:

> *"The informal group shall review the requirements and limitations associated with **Automatically Commanded Steering Function technology (ACSF)** as defined in Regulation No. 79. It shall prepare a draft regulatory proposal regarding advances in control system technology and the transport opportunities provided by the Vienna and Geneva Conventions."*

The work of the ACSF group is very important for the European Union as the EU replaced its own steering system directive by UN Regulation No. 79 in 2009 and made it compulsory for the EU type-approval of vehicles.

Since the last major amendment to Regulation 79 in 2005, much progress has been made by manufacturers on the development of Automatically Commanded Steering Functions (ACSF). The speed limit of 10 km/h for ACSF cannot be justified any longer, provided that adequate requirements are put in place to ensure a safe design of these systems. It should, however, be remembered that in the event that technology advances quicker than the UN Regulation, a special approval scheme is already available in the EU legislation to allow the approval of new technologies not covered by legislation on the basis of an ad-hoc safety assessment (Article 20 of Directive 2007/46/EC on the approval of motor vehicles).

Finally there is an urgent need to clarify the requirements that shall apply to corrective steering systems as many of these systems are now available on the market and lane keeping assist systems are one of the measures that were considered potentially cost/beneficial for mandatory implementation by the assessment report of the general safety regulation (Regulation (EC) 661/2209)[1] and hence taken forward for closer assessment during the course of the currently ongoing TRL project 'General Safety 2 – Analysis of the identified measures and features regarding the way forward for vehicle safety in the EU' (to finish early 2017).

The objective of this project was:

to provide support for amendments to UN Regulation 79 to allow the approval of Automatically Commanded Steering Functions (ACSF), in particular Lane Change Assist (LCA) and enhanced Lane Keep Assist Systems (LKAS).

To meet this objective the following tasks were performed:

1. State of the art review.
    - The objective of this task was to assess automated steering technology and review likely future systems.
2. Best practice with respect to regulation of complex automated systems in other industries / sectors
    - The objective of this task was to review safety testing processes used in other industrial sectors including rail, nuclear and aviation, as well as

[1] Hynd et al. 2015. Benefit and Feasibility of a Range of New Technologies and Unregulated Measures in the fields of Vehicle Occupant Safety and Protection of Vulnerable Road Users. http://bookshop.europa.eu/en/benefit-and-feasibility-of-a-range-of-new-technologies-and-unregulated-measures-in-the-field-of-vehicle-occupant-safety-and-protection-of-vulnerable-road-users-pbNB0714108/

automotive, to ensure that the approaches to managing safety in these areas inform the approach applied in Regulation 79

3. Review current ACSF IWG proposal
    - The objective of this task was to review the current ACSF IWG proposal, identify any potentially safety-relevant issues and make initial recommendations of how they may be resolved.
4. Identify additional requirements to ensure the system functionality is safe in all real world driving scenarios
    - The objective of this task was to propose additional requirements to help resolve the issues identified in task 3 above.

In addition, a separate task (task 5) was performed to provide options for type-approval arrangements that could apply to vehicles undergoing Over-the-Air (OTA) updates after gaining type-approval, where the updates materially change the characteristics or performance of the vehicle or its safety systems.

The results of each of the tasks were as follows:

Task 1: State of the art review

State of the art and proposed corrective steering function (CSF) and ACSF systems were reviewed using information publicly available. A comparison of the functionality of proposed ACSF implementations was made for the following systems:

- Mercedes-Benz Lane Change Assist
- Tesla Autopilot
- Volvo IntelliSafe Autopilot

Task 2: Best practice with respect to regulation of complex automated systems in other industries / sectors

The review of safety testing processes in other industries (railway, nuclear, process, machine and aviation) found that the main standards were, in principle, similar to the automotive industry, mainly because they were all derived from IEC 61508, with the exception of the aviation industry. IEC 61508 sets out a generic approach for electrical/electronic/programmable electronic systems used to perform safety functions, which consists of the following:

- Hazard identification and risk assessment
- Setting of safety requirements (goals)
- Verification of safety requirements

The main standard for the aviation industry, namely DO-178C, was not derived from IEC 61508. Even so, its approach is often similar; for example, for safety requirements and their verification both IEC 61508 and DO-178C use the concept of Safety Integrity Levels (SILs) although DO-178C calls them Design Assurance Levels (DALs). However, DO-178C does not contain guidance for identification of safety hazards; in DO-178C hazards are considered to be caused by software behaviour inconsistent with specified requirements.

From a point of view of assuring the safety of electrical/electronic/programmable electronic systems, the review above clearly shows that an assessment of the development life cycle (including processes and standards followed and verification of safety requirements (goals)) is needed as part of the regulatory requirements.

Key aspects of a regulatory assessment should include:

- Hazard identification and risk assessment with focus on controllability and consideration of human factors in particular the Human Machine Interface (HMI)
- Management of safety requirements, in particular their verification.

From a regulatory point of view, the certification process of aircraft is similar to that for cars in that they both use a type-approval (certification) process. However, there are some notable differences:

- For aircraft the process is defined in much greater detail by direct reference to the use of certain standards in 'Acceptable means for compliance (AMC)' documents. For software development AMC 20-115C recommends directly the use of DO-178C. In contrast for automobiles no direct recommendations for use of specific standards are made for software development, although ISO 26262 appears to be becoming the norm.
- For aircraft the process often takes much longer; compliance demonstration may be greater than five years for large aircraft; for automobiles it is usually much less than a year.

Task 3: Review current ACSF IWG proposal

A review of the current ACSF IWG proposal (Informal documents: ACSF-06-28 and ACSF-07-20), was performed with a focus to ensure safe system function in all real-world driving situations. To ensure a complete and consistent review, each CSF and ACSF category was reviewed with consideration of the following:

- Safety under normal operating conditions
- Safety under fault conditions
- Driver monitoring / system misuse
- Driver information
- Transition demand and related safety manoeuvres
- Incidents

The following four major issues were identified:

1. Inconsistent interpretation and application of CEL Annex (Annex 6)
2. Safety under all real-world scenarios (operational safety), in particular for higher category (B2, E) ACSF systems.
3. Driver monitoring (The driver's role when using ACSF)
4. In-service safety performance

Further work to address these issues was performed in Task 4 and recommendations for the way forward made (see below). Recommendations to address the other (less major) issues identified are given as part of the Task 3 review.

Task 4: Identify additional requirements to ensure the system functionality is safe in all real world driving scenarios

Review of the current ACSF IWG proposal in Task 3 highlighted four major issues. Work reported in this section developed proposals to address each of these issues as follows:

1. Inconsistent interpretation and application of CEL Annex (Annex 6)
    - Currently, the Annex 6 assessment process is not applied in a consistent manner across technical services. **Current 'best practice' application has been identified and amendments to Annex 6 proposed to implement it**. The elements of best practice identified for inclusion within Annex 6 were:
        - Early involvement of the technical service in the development process to ensure good understanding of safety approach and concept
        - 'Audit' of confidential documentation provided, usually performed on site at the OEM, or if necessary at the supplier. Audit should include:
            - Inspection of safety approach at both concept (e.g. HAZOP) and system level (e.g. FMEA, FTA). Check existence of documents/files, their history and (to a certain extent) the content of the documents/files.
                - Note: safety approach at concept level should include consideration of:
                    - Risks driven by interaction of CEL system with other vehicle systems, e.g. effect of LKA on AEB and/or ACC
                    - Risks driven by reasonably foreseeable misuse by driver
        - Traceability of work performed by technical service to level that would allow work to be repeated, e.g. versions of documents inspected are coded and listed

- Resistance to environmental influence, type and scope of tests on climate and mechanical resistance and electromagnetic compatibility should be inspected
- Possibly, include report template to assure all aspects addressed; an example of a template produced by the German approval authority KBA is available publicly for information.

2. Safety under all real-world scenarios (operational safety)
   - For lower category systems (CSF and B1) the current ACSF IWG proposal requires 'hands-on' operation. Physical contact with the steering wheel is an important prerequisite to enable a driver to react promptly to the driving environment. Enforcement of steering wheel contact will also give conscientious drivers a strong indication of the expectation put on them to permanently remain in control of the vehicle. (However, in TRL's view, hands-on detection alone may not prevent all foreseeable misuse: see related recommendations on driver monitoring below). **On this basis, in the short term, TRL recommend that no additional requirements for operational safety are necessary for lower category systems (CSF and B1). However, in the longer term, additional requirements for driver monitoring should be considered for some B1 systems, especially if a regulation dedicated to driver monitoring is developed.**
   - For higher category systems (B2 and E), the current proposal permits 'hands-off' operation and also allows a period of up to about three minutes in which the driver may be 'out of the loop' and may not be monitoring the environment. Therefore, for this period the system must be capable of controlling the vehicle. Hence, **for higher category systems (B2 and E) TRL recommend that requirements similar to those for an SAE Level 3 system should be imposed**, i.e. a comprehensive assessment to assure safe operation in the full range of real-world conditions which may occur in the operational design domain (ODD) is required. An initial list of requirements has been developed.
   - These requirements could be implemented within Regulation 79 or more logically in a new horizontal regulation for automated vehicles.

3. Driver monitoring:
   - TRL's review of the draft working documents identified some issues with the currently included driver monitoring requirements ('hands-on detection' for Category B1 systems; 'driver activity detection' for Category B2 systems):
     - Hands-on detection alone leaves room for potential misuse of Category B1 systems (e.g. phone-related activities using one hand). **In the short term, this should be evaluated and addressed by manufacturers during system development (HAZOP to cover foreseeable misuse), and this step of the OEM should be checked by the technical service during the Annex 6 assessment if TRL's proposed changes to the Annex are implemented.**
     - **In the longer term, however, it is recommended that consideration should be given to development of additional, specific driver monitoring requirements in order to ensure a similar standard of misuse prevention between different systems.** The current draft monitoring requirements for Category B2 systems are considered by TRL too unspecific and underdeveloped to ensure safe operation. Additional regulatory work will be required to develop appropriate requirements. These should ideally be placed into a horizontal regulation that can be called upon by different regulations and can be updated and developed further independently of other technology domains related to automated driving, such as steering systems.
   - TRL's technology review of driver monitoring technologies and system implementations found that the technology exists to detect and react to the three main driver states considered during this review (fatigue, distraction and

inattention). Going beyond simple hands-on detection, the most prominent technology appears to be centred on the use of driver-facing infrared cameras.
    - Each of the systems would need to be tested in the specific scenario in an autonomous driving context. For example, in SAE Level 3, a driver could engage in other tasks. Further research would need to establish with a high degree of certainty whether eye or head position systems could detect and distinguish, for example, between a driver looking down at a mobile phone and being asleep.
4. In-service safety performance
    - For the way forward, it is interesting to consider the strategy for implementation of the regulatory measures proposed above, especially for higher category systems (B2 and E). For these systems there is, as yet, no known mechanism or test that allows technical services to fully validate at the time of type-approval at a reasonable cost that the system will perform safely in all real-world scenarios that it may encounter. Instead the approach being developed is to check a limited number of scenarios and aspects of the system development process, in particular the safety concept. It is therefore reasonable to assume an increasing potential for safety relevant issues in products which are not detected during type-approval in the future. To help counter this, clarification will be needed that manufacturers will bear the full responsibility for their products (e.g. **by a self-declaration on the safety of their product) and/or in-service safety performance monitoring coupled with recall action to address any safety issues identified could be implemented**.
    - From a strategy point of view, the aim is to ensure safe performance of ACSF in all real-world conditions. This can be achieved by adding more scrutiny up-front (e.g. requirements for operational safety) and/or ensuring that safety issues in real-world use are detected and resolved early (e.g. in-service safety performance). The interesting question in terms of strategy is should both approaches be used and if yes, what balance of the two approaches should be used.
    - At this stage it is not possible to answer this question definitively. However, on the basis that it is proposed to use both approaches in the US Federal Automated Vehicles Policy, it would appear sensible that **measures should be put in place in UN Regulation to enable the use of the three approaches (enhanced requirements for operational safety checked by authorities at type-approval level, self-declaration by the manufacturer on some design aspects and proactive in-use safety monitoring)**. From the point of view of amendments to Regulation 79, this would entail introducing requirements for the collection of, "*event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues*", for higher category ACSF systems (i.e. B2, E). To achieve this it is recommended that regulatory requirements are expanded to include collection of data for events, incidents and road accidents sufficient for use to establish the cause of any such issues and any related system defects. It should be noted that some of these data may be subject to the European data protection rules (Regulation and Directive) and therefore an agreement may need to be established between the customer and the OEM to allow collection and subsequent processing, and clarify the question of data ownership.

Task 5: OTA updates

OTA software / firmware updates have the potential to offer large benefits to the automotive industry due their capacity make software updates easier and thus potentially increase customer satisfaction and completion rates, in particular for recalls linked to cyber security issues.

However, if OTA updates are used to upgrade functionality, especially if the system update provides a new function subject to type-approval which was not initially type-

approved, this may cause safety or emissions problems and make the vehicle not compliant with its initial type-approval and its registration certificate.

From a regulatory point of view, OTA updates of pre-registered/production vehicles affecting approved functions could follow the current practice for a type-approval update. Manufacturers would have to inform the type-approval authorities about changes that affect a type-approved system (i.e. steering function in the case of Regulation 79) and the type-approval authorities would have to decide if such changes should be considered as a revision/extension or as a new type-approval. For Regulation 79, this may require the change of the type definition as today it does not include the category of ACSF with which the steering function is equipped.

Post-registration/production OTA updates on used vehicles create more challenges regarding harmonisation, because modifications to registered vehicles are covered by national legislation and not EU rules. These challenges could lead to a different legal treatment of OTA updates across the EU. In order to ensure a coherent approach around the EU and decrease the burden on manufacturers and vehicle owners, the EU type-approval framework could be extended to manage software updates that could affect approved systems of used vehicles in a similar way as there are today UN regulations on the retrofitting of LPG/CNG vehicles or for replacement parts. Relevant software updates could be validated by type-approval authorities (this may require new testing, e.g. in case of change of functions). Then the update could be deployed by the manufacturer entirely under the manufacturer's responsibility and/or in combination with an individual approval/periodic technical inspection (PTI) depending on the scope of the update.

For updates deployed purely under the manufacturer's control, the question of responsibility should be clarified because today under most of national rules, it is the vehicle owner who is responsible for maintaining the vehicle in compliance with the relevant legislation. It may also be difficult to check remotely that the updated vehicles still meet the approval requirements. This may lean in favour of a solution of limiting the OTA updates to non-critical functions and require a physical inspection (by the manufacturer, authorities) for critical functions. Software updates not impacting the type-approved functions could be left out from the type-approval framework.

Software / firmware versions of safety and environmental systems could also be checked at PTI to ensure that vehicle has received all appropriate updates and has not been tampered with. The Implementing Act for Directive 2014/45/EU may offer an opportunity to implement this, if appropriate information was to be included within the technical information that manufacturers are obliged to supply to PTI authorities for inspection purposes. Discussions, led by the European Commission's DG Move, on what to include in the Implementing Act are ongoing at present. However, it should be recalled that the first PTI only occurs after a number years (after 4 years for cars in many member states).

Cyber-security is still a major issue and much work is being performed on it at present, for example the guidelines being prepared by the WP.29 ITS/AD working group. Until security issues are resolved, it will probably not be possible to perform OTA updates for safety and/or environmental vehicle systems.

1 Introduction

The objective of the United Nations (UN) World Forum for Harmonisation of Vehicle Regulations (WP.29) is to initiate and pursue actions aimed at the development or worldwide harmonisation of technical regulations for vehicles. WP.29 currently administers three UN agreements, namely the 1958, 1998 and 1997 agreements. The 1958 agreement concerns the adoption of uniform technical prescriptions on equipment and parts which can be fitted and/or be used on wheeled vehicles (i.e. UN(ECE) Regulations) and the conditions for reciprocal recognition of approvals. The 1998 agreement concerns the establishment of global technical regulations (i.e. UN GTRs) and the 1997 agreement adoption of uniform conditions for periodical technical inspection.

WP.29 has a subsidiary body, the Working Party on Brakes and Running Gear (GRRF), dedicated to the preparation of regulatory proposals on active safety, braking and running matters. As part of this technical area there is an Informal Working Group (IWG) which is considering Automatically Commanded Steering Functions (ACSFs). Initiated in February, 2015; the Terms of Reference for this group (Informal Document ACSF-01-02) begin with the requirement that:

> *"The informal group shall review the requirements and limitations associated with **Automatically Commanded Steering Function technology (ACSF)** as defined in Regulation No. 79. It shall prepare a draft regulatory proposal regarding advances in control system technology and the transport opportunities provided by the Vienna and Geneva Conventions."*

The IWG shall address the following issues:

- Review the current speed limitation (10km/h) with the purpose of permitting ACSF functionality during urban and interurban journeys
- Define requirements for communicating to the driver a malfunction of ACSF
- Define requirements to enable evaluation of the ACSF during periodic technical inspection

The target completion date for the IWG's work was set as February 2017.

UN Regulation No. 79 concerns the approval of vehicles with regard to steering equipment. It establishes uniform provisions for the layout and performance of steering systems fitted to vehicles used on the road.

In its scope, the regulation includes Advanced Driver Assistance Steering Systems, whereby the driver remains in primary control of the vehicle but may be helped by the steering system being influenced by signals initiated on-board the vehicle. As described in the regulation:

> *"Such Systems can incorporate an "Automatically Commanded Steering Function", for example, using passive infrastructure features to assist the driver in keeping the vehicle on an ideal path (Lane Guidance, Lane Keeping or Heading Control), to assist the driver in manoeuvring the vehicle at low speed in confined spaces or to assist the driver in coming to rest at a pre-defined point (Bus Stop Guidance)."*

The construction provisions stipulate that:

> *5.1.6.1 Whenever the ACSF becomes operational, this shall be indicated to the driver and control action shall be automatically disabled if the vehicle speed exceeds the set limit of `10 km/h by more than 20 per cent or the signals to be evaluated are no longer being received. Any termination of control shall produce a short but distinctive driver warning by a visual signal or by imposing a tactile warning signal on the steering control.*

It also explicitly defines that:

> *"Advanced Driver Assistance Steering Systems can also incorporate a "Corrective Steering Function" that, for example, warns the driver of any deviation from the chosen lane (Lane Departure Warning), corrects the steering angle to prevent*

departure from the chosen lane (Lane Departure Avoidance) or corrects the steering angle of one or more wheels to improve the vehicle's dynamic behaviour or stability."

These requirements present a regulatory barrier to an ACSF. Effectively, they prevent the approval of ACSF, such as enhanced lane keep assist (i.e. lane keep assist with lane centring) and lane change assist, that operate above 12 km/h (10 km/h plus 20%).

It is interesting to note that in the first meeting of the ACSF IWG, provisional guidance to GRRF from WP.29 was presented (Informal Document ACSF-01-11). This included

- Technologies to be considered in the scope of Vienna and Geneva Conventions
- Concept of "designed to assist drivers"
- Possible targeted systems
- Possible items to be provided in the regulation

Although still under discussion, technologies that were considered to be in the scope of Vienna and Geneva Conventions were partial automated 'assistance' systems functioning under the specific command of the driver. Examples of these were given as lane keeping and lane changing operation 'designed to assist drivers' in a restricted area which has multilane road sections with constructional separation of the two directions of traffic and no mixed traffic with pedestrians, cyclists and oncoming vehicles.

The work of the ACSF group is very important for the European Union as the EU replaced its own steering system directive by UN Regulation No. 79 in 2009 and made it compulsory for the EU type-approval of vehicles.

Since the last major amendment to Regulation 79 in 2005, much progress has been made by manufacturers on the development of Automatically Commanded Steering Functions (ACSF). The speed limit of 10 km/h for ACSF cannot be justified any longer, provided that adequate requirements are put in place to ensure a safe design of these systems. It should, however, be remembered that in the event that technology advances quicker than the UN Regulation, a special approval scheme is already available in the EU legislation to allow the approval of new technologies not covered by legislation on the basis of an ad-hoc safety assessment (Article 20 of Directive 2007/46/EC on the approval of motor vehicles).

Finally there is an urgent need to clarify the requirements that shall apply to corrective steering systems as many of these systems are now available on the market and lane keeping systems are one of the measures considered to be cost/beneficial for safety by the assessment report of the general safety regulation (Regulation (EC) 661/2209)[2].

The objective of this project was:

to provide support for amendments to UN Regulation 79 to allow the approval of Automatically Commanded Steering Functions (ACSF), in particular Lane Change Assist (LCA) and enhanced Lane Keep Assist Systems (LKAS).

To meet this objective the following tasks were performed:

1. State of the art review
    - The objective of this task was to assess automated steering technology and review likely future systems.
2. Best practice with respect to regulation of complex automated systems in other industries / sectors
    - The objective of this task was to review safety testing processes used in other industrial sectors including rail, nuclear and aviation, as well as

[2] Hynd et al. 2015. Benefit and Feasibility of a Range of New Technologies and Unregulated Measures in the fields of Vehicle Occupant Safety and Protection of Vulnerable Road Users. http://bookshop.europa.eu/en/benefit-and-feasibility-of-a-range-of-new-technologies-and-unregulated-measures-in-the-field-of-vehicle-occupant-safety-and-protection-of-vulnerable-road-users-pbNB0714108/

automotive, to ensure that the approaches to managing safety in these areas inform the approach applied in Regulation 79

3. Review current ACSF IWG proposal
    - The objective of this task was to review the current ACSF IWG proposal, identify any potentially safety-relevant issues and make initial recommendations of how they may be resolved.
4. Identify additional requirements to ensure the system functionality is safe in all real world driving scenarios
    - The objective of this task was to propose additional requirements to help resolve the issues identified in task 3 above.

In addition, a separate task (task 5) was performed to provide options for type-approval arrangements that could apply to vehicles undergoing Over-the-Air (OTA) updates after gaining Type-approval where the updates materially change the characteristics or performance of the vehicle or its safety systems.

The results of these tasks, which generally build upon each other, are reported in the sections below.

2 Task 1: State of the art review

2.1 Introduction

The objective of this task was to assess automated steering technology and review likely future systems. UN Regulation No. 79 in its current version (Revision 2) draws a line between two main categories of systems that can influence the steering: Corrective steering functions (CSF) and automatically commanded steering functions (ACSF).

CSF is currently defined as:

> *"Corrective steering function" means the discontinuous control function within a complex electronic control system whereby, for a limited duration, changes to the steering angle of one or more wheels may result from the automatic evaluation of signals initiated on-board the vehicle, in order to maintain the basic desired path of the vehicle or to influence the vehicle's dynamic behaviour.*
>
> *Systems that do not themselves positively actuate the steering system but that, possibly in conjunction with passive infrastructure features, simply warns the driver of a deviation from the ideal path of the vehicle, or of an unseen hazard, by means of a tactile warning transmitted through the steering control, are also considered to be corrective steering."*

ACSF are currently defined as:

> *"Automatically commanded steering function" means the function within a complex electronic control system where actuation of the steering system can result from automatic evaluation of signals initiated on-board the vehicle, possibly in conjunction with passive infrastructure features, to generate continuous control action in order to assist the driver in following a particular path, in low speed manoeuvring or parking operations.*

UN R79 currently demands that ACSF must be disabled at vehicle speeds above 12 km/h (i.e. 10 km/h plus 20 percent), effectively limiting this category to parking and other low speed applications.

The ACSF informal working group is developing amendments to the regulation which will shift the exact borderline between the definitions of these categories and will lift the general speed restriction to allow certain new ACSF applications (see section 4). While precise detail of these changes is still under discussion, the following sub-sections give examples of systems that might be approved as CSF and ACSF in the future to give an overview of the state of the art of automated steering technology and likely future systems in these categories.

2.2 Corrective steering functions (CSF)

A CSF is a system that influences dynamic behaviour of a vehicle by changing the steering angle discontinuously. It can be used to help improve the vehicle handling performance, efficiency and to help prevent loss of stability caused by factors such as μ-split, side wind, etc.

CSF could, for example, help in the following circumstances:

- Driver's effort in the steering wheel to fight against side wind (e.g. for HGVs with large lateral surface) and improve transition from high to low / low to high side wind, e.g. when overtaking a truck.
- Improve vehicle dynamic behaviour by adapting the four-wheel steering system according to the speed, lateral acceleration and steering control angle.
- Increase the efficiency of ABS, ESC or traction control.
- Improve steering interventions to help traction control e.g. on low friction gradients, to prevent unstable drive axle lateral drift on e.g. tractor-semi-trailer combinations.

Listed below are some of the potential safety functions:

- Steering Support Programme (SSP) – An electronic power steering programme that helps maintain active safety of the vehicle. This system couples together electronic stability control (ESC) and electronic power steering (EPS). An example of this is shown below in Figure 1, where a vehicle is performing an emergency stop on a split-μ surface (the left side tyres are on a dry road and right side tyres on an icy road). The electronic power steering programme will no longer limit the braking on the left wheel but will apply a small amount of torque to the steering wheel to assist the driver correct the vehicle trajectory. The driver still remains in control of the vehicle.

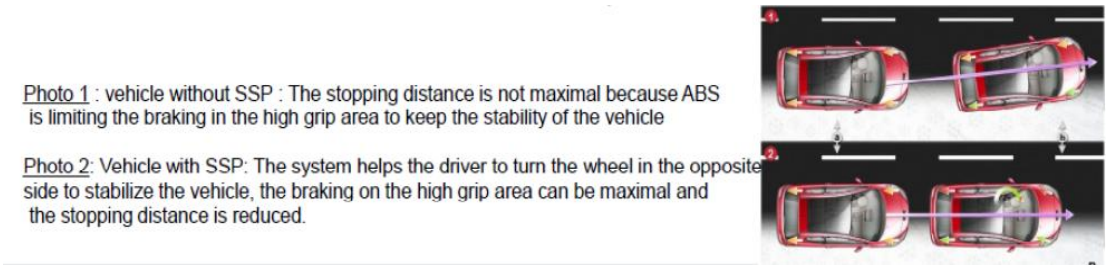

Figure 1: Functionality of steering support programme (SSP) in μ-split braking situation. (OICA, 2016)

- Evasive emergency steering assist system - A system that adds a precise amount of torque to support the movement of the steering wheel should the driver initiate an evasive manoeuvre or lose control of the steering as shown in Figure 2.

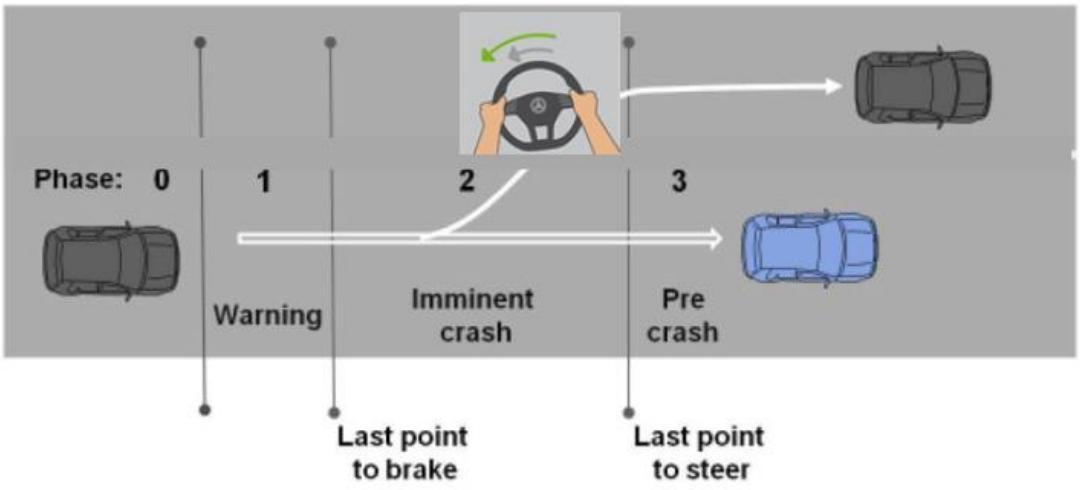

Figure 2: Evasive emergency steering assist. (OICA, 2016)

- Run-off road system: A system mainly fitted to trucks, as shown in Figure 3, that applies a steering correction to enable a single manoeuvre to bring the vehicle back in lane **after** it has crossed the lane markings (e.g. when a vehicle is about to leave the road or hit a road safety barrier). Note that the Lane Departure Warning System (LDWS), which is mandatory for trucks, will give a warning (usually haptic) after the lane marking is crossed.

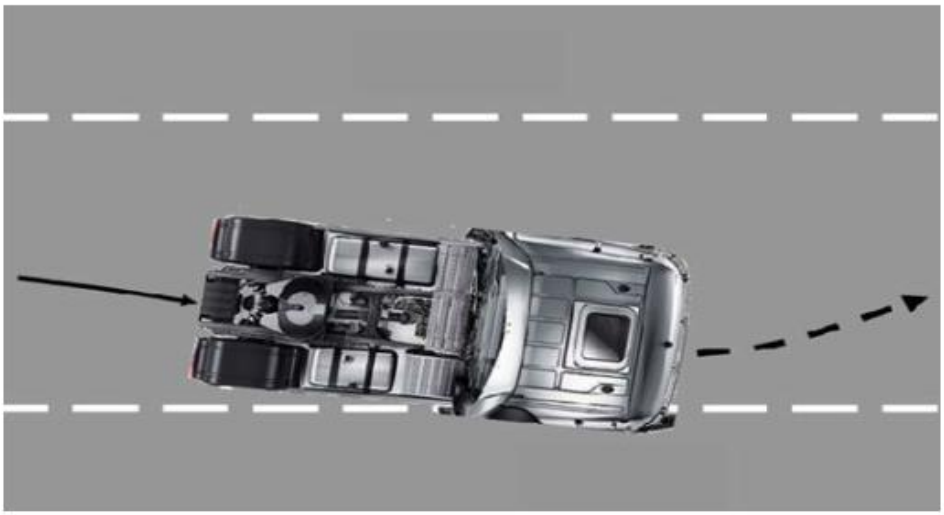

Figure 3: Run-off road system. (OICA, 2016)

2.3 Automatically commanded steering functions (ACSF)

This section focuses on new and emerging technologies that actively exercise lateral control of the vehicle at speeds above 12 km/h and might thus be affected by the prescriptions of UN R79 for ACSF.

Several OEMs have released a technology with the moniker of Lane Change Assist or Assistant/Assistance in the past. It should be noted that these functions can be quite different from one another and often only alert the driver about vehicles approaching in adjacent lanes (e.g. blind spot warning) rather than actively controlling of the vehicle. Examples of warning-only systems are Porsche Lane Change Assist, Volkswagen Lane Change Assistant Side Assist or Volvo Blind Spot Information System. It should be noted that these warning-only systems are not within the scope of Regulation 79.

2.3.1 Lane Keeping Aid / Assist System

Description

This can be defined as a system which forecasts the straying of the vehicle out of the lane and gives a warning, sometimes haptic, e.g. vibration of steering wheel, and applies a light corrective steering torque to help the vehicle stay in the lane **before** it leaves the lane. The system is primarily intended for motorway or other major roads, is activated only above a minimum speed (e.g. 40 mph) and requires drivers to have their hands on the steering wheel. Such a system is illustrated below in Figure 4.

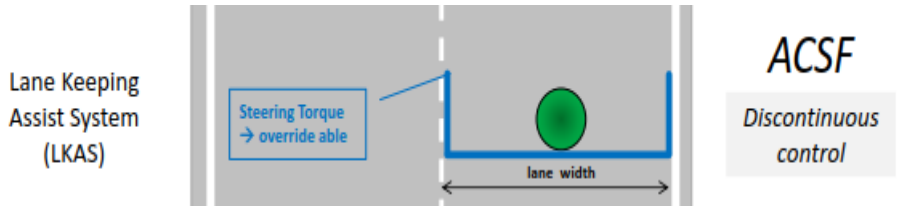

Figure 4: Lane Keeping Aid / Assist System. (OICA, 2016)

System category

Currently this system is classified as a CSF. However, this system is likely to be classified as Category B1 ACSF in the future amendments of UN R79 (according to the definition in the ACSF-Document No.06-28 and discussions in the 7th meeting).

2.3.2 Lane Guidance (Assist) System

Description

This can be defined as a system which applies continuous torque and control to keep the vehicle in the centre of the lane. This system is not permitted by Regulation 79 at present. It is meant **only** for use on motorways and other major type roads with physical separation between traffic in different directions. It may also be used with hands-off the steering wheel, although the driver will be expected to monitor the system and be in a position to take over control if required. Such a type of system is illustrated below in Figure 5.

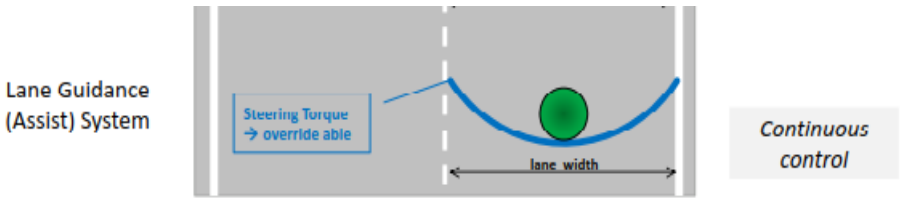

Figure 5: Lane Guidance (Assist). (OICA, 2016)

System category

The system is likely to be classified as Category B2 ACSF in the future amendments of UN R79 (according to the definition in the ACSF-06-28 and discussions in the 7th meeting).

Timescales

Hands-on versions of this system are market ready as illustrated by Mercedes Benz Active Lane Change Assist – see section below.

2.3.3 Mercedes-Benz Active Lane Change Assist

Description

Lane Change Assist is a function which has been developedfor Mercedes-Benz's technology suite 'Intelligent Drive'.

The system performs a lane change manoeuvre to overtake vehicles on dual carriageways. A positive action by the driver is required to initiate the lane change (applying the indicator for longer than two seconds). The system allows lane changes in both directions: offside and nearside lane, for overtaking and re-joining the initial lane, respectively.

System category

The system is likely to be classified as Category C ACSF in the future amendments of UN R79 (according to the definition in the ACSF-06-28).

A car with this system will likely be classified as SAE Level 2 automated vehicle (according to SAE J3016[3]), because, most likely, it will be bundled with ACC and thus provide simultaneous lateral and longitudinal control of the vehicle under driver supervision.

Timescales

The system was introduced onto the market with the new E-class in 2016.

Sensor and actuator technology

The system uses mid-range radar for rear and side vehicle detection, and forward-facing long-range radar sensors and a stereo camera.

The system steers by direct application of a steering torque and does not use one-sided braking.

Technology bundles

The system will probably be bundled in a package with AEB, ACC and LKA.

Operating conditions

The system operates under the following conditions:

- Road type: Dual carriageways (two or more lanes with traffic flowing in the same direction)
- Adjacent lane detected by camera via lane markings
- Steering Pilot (active lane keeping) is activated
- Driving speed between 80–180 km/h
- No vehicle detected in a defined zone in adjacent lane behind and to the side of the vehicle (allowing a lane change within three seconds)
- Activation: Driver applies turn signal for longer than two seconds

Safety function and limitations

The system can be overridden by the driver at any point via steering or braking.

The driver has to perform a positive action to initiate a lane change. TRL is not privy to details of how the system deals with a situation where the driver commands a lane change and a vehicle is approaching from behind at high speed. Assuming a maximum differential speed of up to 170 km/h on German motorways (80 km/h minimum operating speed of Lane Change Assist; 250 km/h highest speed limitation of most high performance cars) and an assumed range of the mid-range radar of 100 metres, an approaching vehicle could cover the system's detection range within approximately 2.1 seconds.

The driver is obliged to supervise the system. The system detects whether the driver's hand are on the steering wheel as an indication of their alertness. The exact conditions (interval of checks, abort conditions, etc.) could not be found in the literature.

It should be noted that the system is intended for use on dual carriageways with traffic flowing in one direction, rather than for overtaking vehicles on single carriageways. Use is limited to these road types via the navigation module (geo-fencing).

2.3.4 Tesla Autopilot

Description

[3] http://standards.sae.org/j3016_201609/

Autopilot is an automated driving function released by Tesla Motors on European cars in 2015.

After being activated by the driver, the system performs longitudinal and lateral control of the car on dual carriageways under permanent supervision of the driver. The longitudinal control is similar to an ACC function with a maximum driving speed set by the driver or dependent on the current speed limit and speed adaptation to preceding traffic. The system also reduces driving speed before bends. The lateral control is a lane following and lane change function. Lane changes (to offside or nearside) are performed only when instructed by the driver (applying the indicator for a certain time).

System category

A car with the Autopilot system would be classified as SAE Level 2 automated vehicle (according to SAE J3016).

The system might be classified as a Category B1 or Category B2 ACSF (depending on hands-on or hands-off requirement) combined with a Category C ACSF (according to the definition in the ACSF-06-28).

Timescales

The system has been deployed to customer's cars in 2015 and is continuously being updated using over-the-air (OTA) updates.

Sensor and actuator technology

The system uses forward-facing radar and camera and 12 long-range ultrasonic sensors (range: approximately 5 metres around the car in every direction at all speeds).

Actuators used are a digitally-controlled electric assist braking system. The actuators used for steering wheel movement are unknown.

Technology bundles

Autopilot capable Tesla models also incorporate AEB functionality and LDW (activated also when not in Autopilot mode).

Operating conditions

- Road type: Dual carriageways (two or more lanes with traffic flowing in the same direction)
- The driver's hands have to remain on the steering wheel

Safety function and limitations

Tesla continuously develops software updates, which are distributed over-the-air to cars in customer's hands. Furthermore, the Autopilot system is described by Tesla as continuously learning. The exact interpretation of this is unknown, but to the authors best understanding, this indicates that the behaviour of a single car will also adapt based on the routes it has previously driven (e.g. learning from situations where the system was overruled by the driver).

The driver is obliged to supervise the driving environment (and has to perform a positive action to initiate a lane change). TRL is not privy to detail of whether and how the driver's alertness is supervised by the car.

The system is intended for use on dual carriageways with traffic flowing in one direction. There is a potential for safety-relevant use case misinterpretation or customer misuse. Current software versions are reported to apply geo-fencing to actively enforce this restriction. Early versions had this restriction explained in the user manual but not enforced via software, and videos on the internet showed drivers misusing the system.

The system does not detect traffic lights.

It is unclear how vehicles approaching from behind at high speed are handled with regard to lane changes, particularly considering the short detection range of the ultrasonic sensors (Tesla does not report using rear-facing radar).

2.3.5 Volvo IntelliSafe Autopilot

Description

IntelliSafe Autopilot is an autonomous driving function that will perform the entire driving task on certain roads. The driver will activate the system and is then allowed to perform other tasks but has to remain available to take over control within a few seconds.

System category

A car with the IntelliSafe Autopilot system would be classified as SAE Level 3 or Level 4 automated vehicle (according to SAE J3016).

The system might be classified as Category B2 ACSF combined with a Category E ACSF (according to the definition in the ACSF-06-28).

Timescales

The system is being actively tested and will be trialled with the general public in 2017. It should be noted that this trial will not involve mass market introduction of the system, unlike the Mercedes and Tesla systems described previously.

Sensor and actuator technology

The system uses four mid-range radars for all-round detection; three long-range radars (one forward-facing, two rear-facing), four cameras for all-round view, a long range forward-facing trifocal camera (including narrow, long-range view), a static forward-facing laser (range: 150 metres), and 12 ultrasonic sensors providing all-round detection.

The system steers by direct application of a steering torque and does not use one-sided braking.

Technology bundles

The system performs the driving task autonomously, so is designed to perform all functions.

Operating conditions

The system is intended for use on carriageways with traffic flowing in one direction. It is assumed that this limitation is enforced via geo-fencing.

Volvo names some conditions where autonomous driving might not be available as: Exceptional weather conditions, technical malfunction, or that the end of the route has been reached.

Safety function and limitations

The driver is not obliged to supervise the system permanently, but has to be available to take over control after a certain period. TRL is not privy to detail of whether the driver's readiness to take over is monitored by the car.

If the driver does not take over control when prompted, the car will perform the minimal risk manoeuvre. This manoeuvre will bring the car to a halt in a safe place, i.e. for example pull away from the main carriageway into a layby.

2.3.6 Comparison of ACSF system functions

The following tables provide an overview of the functionality (Table 1) and sensor equipment (Table 2) of the ACSF implementations discussed above. They summarise information given in more detail in the preceding sub-sections.

Table 1: Overview of functionality of proposed ACSF implementations

System name	SAE Level	ACC (adaptive to traffic)	ACC (adaptive to speed limit)	ACC (adaptive to road geometry)	Autonomous emergency braking	Lane following	Lane changing (at driver's command)	Lane changing (autonomous)	Autonomous emergency steering	Driver monitoring	Minimal risk manoeuvre
Mercedes-Benz Lane Change Assist	**2**	x	?	?	x	x	x	–	?	x	x
Tesla Autopilot	**2**	x	x	x	x	x	x	–	?	?	?
Volvo IntelliSafe Autopilot	**3/4**	x	x	x	x	x	–	x	?	?	x

Table 2: Overview of sensor equipment of proposed ACSF implementations

System name	Sensors forward	Sensors rear	Sensors side	Sensors all-round
Mercedes-Benz Lane Change Assist	Mid-range radar, long-range radar, camera	Mid-range radar	Mid-range radar	–
Tesla Autopilot	Radar, camera	–	–	Long-range ultrasonic
Volvo IntelliSafe Autopilot	Mid-range-radar, long-range radar, trifocal camera, laser (static)	Mid-range-radar, long-range radar	Mid-range-radar	Cameras, ultrasonic

Table 3 provides an overview of typically achievable maximum detection ranges of state-of-the-art versions of different sensor technologies. The exact capabilities of the sensor models employed for the ACSF implementations above are not known to TRL.

Table 3: Typical maximum detection ranges of various sensor technologies

Sensor technology	Approximate maximum range
Ultrasonic transceiver	~8 metres
Short-range radar	~50 metres
Mid-range radar	~160 metres
Long-range radar	~250 metres
Lidar/laser (static)	~150 metres
Camera (pedestrian detection)	~30 metres
Camera (vehicle detection)	~200 metres

3 Task 2: Best practice with respect to regulation of complex automated systems in other industries / sectors

3.1 Introduction

The objective of this task was to review safety testing processes used in other industrial sectors including rail, nuclear and aviation, as well as automotive, to ensure that the approaches to managing safety in these areas inform the approach applied in Regulation 79.

Safety can be defined as freedom from unacceptable risk of physical injury or of damage to the health of people, either directly or indirectly as a result of damage to property or to the environment.

Functional safety is a part of overall safety that depends on a system or equipment operating correctly in response to its inputs.

Neither safety nor functional safety can be determined without considering the systems as a whole and the environment with which they interact. Generally, the process for functional safety is as follows:

- The significant hazards for equipment and any associated control system in its intended environment are identified by the specifier or developer via a hazard analysis.
- A risk analysis is performed to determine whether functional safety is necessary to ensure adequate protection against each significant hazard. If so, then it has to be taken into account in an appropriate manner in the design.

It should be noted that functional safety is just one method of dealing with hazards, and other means for their elimination or reduction, such as inherent safety through design, are also of primary importance.

The development of hardware and embedded software requires both high efficiency (to minimise costs) and great caution because errors could have disastrous safety consequences. Currently, in the automotive industry, the emphasis in software development is around faster delivery and increased functionality. To achieve this it is important that sound engineering practices around the software development lifecycle are followed. Furthermore achieving functional safety in software requires that exacting engineering principles be implemented:

- Functional safety must be proactive
- Processes must be controlled, measured, and repeatable.
- Defects should be prevented through the implementation of standards.
- Testing (verification) must be effective and deterministic.
- Testing should be done for complex memory problems.

The following items form the basis of the development of safe systems:

- Development life cycle
- Processes and standards
- Verification methods (including software tests).

3.2 Development life cycle

Development needs the choice of a life cycle. Typical examples are the Waterfall cycle, V cycle, W cycle, prototype life cycle, spiral life cycle, incremental life cycle, Lean Software Development and Agile.

The most relevant cycles for the automotive industry are the V and W cycles because these are used in ISO 26262 (Figure 6), which is used widely in the automotive industry.

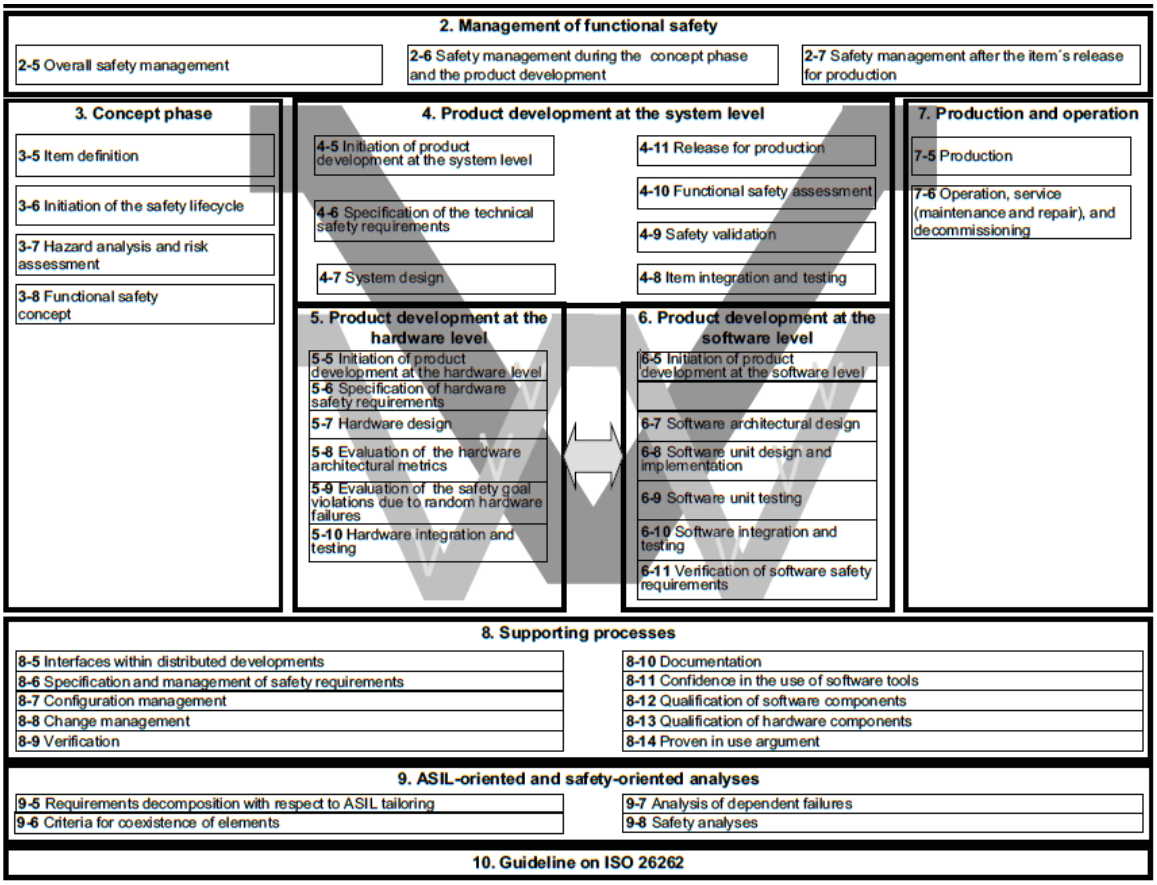

Figure 6: Overview of ISO 26262 – management of functional safety – showing use of V and W cycles.

The V and W cycles were developed from the waterfall cycle. Each of these cycles is described briefly below.

3.2.1 Waterfall cycle

The waterfall development life cycle is a sequential life cycle first formally described by Winston Royce in 1970 (Royce, 1970):

1. Needs, 2. Design, 3. Implementation (Solution building and module integration), 4. Verification (Tests and installation), 5. Maintenance.

The sequential nature of this life cycle is both its main strength and weakness. The life cycle's needs must be stable otherwise the life cycle is disturbed and frequent loops become necessary, which harms the effectiveness of the model. This makes it unsuitable for projects whose specifications will evolve, such as those that are innovative (e.g. only partial specification available at start of project), or include a man-machine interface.

3.2.2 V (and W) cycles

The V cycle is an adaptation of the waterfall model that has similar stages but separates definition / specification activities from test / verification ones and emphasizes the parallelism that can result from this, i.e. as soon as specifications are ready, it is possible to start working on the verification activities (Figure 7). System specification is necessary when the system consists of several products connected. Similarly product specification is needed when the product consists of a number of components, for example software, an electronic board and mechanical components.

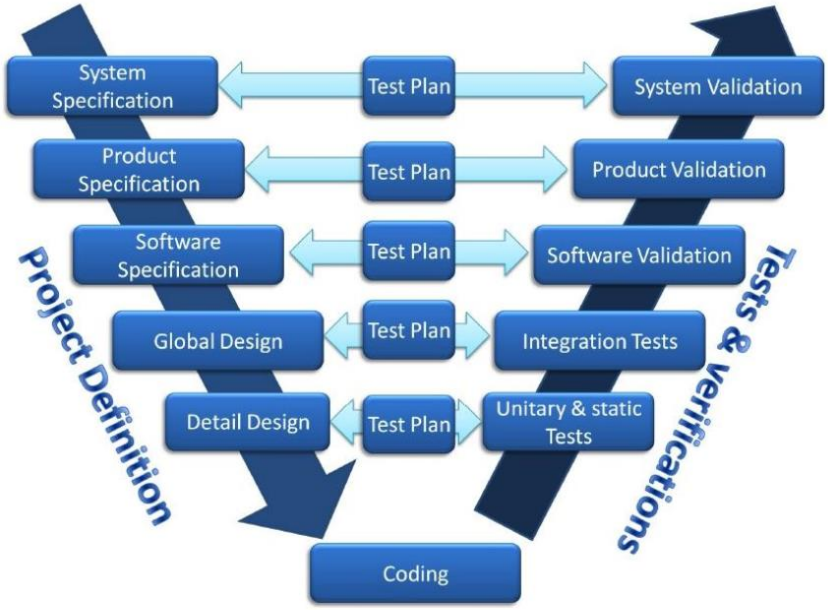

Figure 7: V cycle.

The shape of the V cycle emphasizes that for each stage of the falling edge, there are some corresponding verifications or tests on the rising edge. This structure helps ensure that stages are not forgotten.

The W cycle is an evolution of the V cycle which introduces an iterative aspect in terms of several small successive V cycles, which can overlap. It can be applied to separate different aspects of the design such as software and hardware (e.g. as in ISO 26262) and /or iteratively develop the product with a new version of the product at the end of each iterative V cycle.

3.3 Processes and standards

There are a number of management processes and standards for the development of safety related items. The more relevant of these are described in the sections below.

3.3.1 Processes

ISO 9001, Capability Maturity Model Integrated (CMMI) SPICE, Automotive SPICE and HIS are described below.

3.3.1.1 ISO 9001

ISO 9001 is related to quality management and organisation. Its purpose is to enable a company to provide products that meet customer and relevant regulatory requirements and improve customer satisfaction through continuous improvement. The concepts on which it is based are:

- Customer oriented
- Leadership, management commitment: effective daily management involvement, management by example
- Staff involvement
- Process management
- System approach
- Continuous improvement
- Factual decision making: orientation of choices and decisions by analysing factual data
- A win-win relationship with suppliers

3.3.1.2 CMMI

Capability and Maturity Model Integrated (CMMI) is a reference model that consists of good practices for the improvement and evaluation of engineering companies. It was initiated by the US Department of Defence, and since 2013 is an institute under the control of the Carnegie-Mellon University. CMMI helps to assess and improve a company's maturity and its deployment of processes. There are two main versions, staged and continuous.

In the staged version, 22 process areas are grouped into five levels of maturity (Table 4). A company can improve a set of related processes incrementally. Achieving a given level requires that all previous levels are achieved and maintained.

Table 4: The five maturity and four capability levels of CMMI.

Level	Maturity	Characteristics	Capability
0			Incomplete
1	Initial	Process unpredictable, poorly controlled	Basic
2	Managed	Process defined for projects and often reactive	Disciplined
3	Defined	Process defined for projects and proactive	Adjusted
4	Quantitatively manged	Process measured and controlled	
5	Optimized	Focus on continuous process improvement	

In the continuous version four capability levels are defined (Table 4). This version allows a company to improve some chosen processes gradually.

3.3.1.3 SPICE (ISO/IEC 15504) and Automotive SPICE

Software Process Improvement and Capability dEtermination (SPICE) referenced as ISO/IEC 15504:2012 is an international software process standard. It was derived from the ISO/IEC 12207 standard lifecycle and maturity models such as CMM, Trillium and Bootstrap.

Capability is rated into six levels by assessment of process attributes and generic practices in six areas: organizational, management, engineering, procurement, support and operations. The 6 levels are:

0: Incomplete process; 1: Performed process; 2: Managed process; 3: Established process; 4: Predictable process; 5: Optimizing process.

Although SPICE is essentially audit orientated, it can still be used for process improvement.

A special version of this standard for the automotive industry is called Automotive SPICE.

3.4 Standards

There are a large number of standards available for various industry sectors for safety related systems which incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices. IEC 61508 is the primary standard for most industries, with the exception of the avionics industry.

IEC 61508 sets out a generic approach for all safety related systems which incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices. Industry specific standards have been developed from and/or are based upon IEC 61508. Examples are:

- ISO 26262 for the automotive industry, specifically passenger cars with a maximum gross up to 3,500 kg.

- IEC 61511 for safety instrumented systems in the process industry sector.
- IEC 61513 for instrumentation and control important to safety in nuclear power plants.
- IEC 62061 for the machine industry.
- EN 50126/EN 50128/EN 50129 for the railway industry.

The standards for the avionics industry DO-178B and C are not related to IEC 61508.

Other standards, which are particularly relevant for software development, include the Motor Industry Software Reliability Association (MISRA) software development best practice guidelines for the C programming language. These guidelines aim to facilitate code safety, security, portability and reliability. They are a widely accepted model for best practices by leading developers for C programming in sectors including, automotive, aerospace, telecom, defence, railway and others. Unfortunately, MISRA standards are not freely available and must be purchased.

The sections below describe IEC 61508, ISO 26262, and the avionics industry standards DO-178B and C.

3.4.1 IEC 61508

3.4.1.1 Introduction

IEC 61508 sets out a generic approach for all safety lifecycle activities for systems comprised of electrical and/or electronic and/or programmable electronic components (electrical/electronic/programmable electronic systems (E/E/PESs)) that are used to perform safety functions. This unified approach has been adopted in order that a rational and consistent technical policy be developed for all electrically-based safety-related systems.

A major objective of this standard was to facilitate the development of application sector standards. Because, as noted above, the railway standards EN 50126, EN 50128 and EN 50129, nuclear standard IEC 61513, process industry standard IEC 61511, machine industry IEC 62061, and automotive standard ISO 26262 were derived from IEC 61508, it can be concluded that this objective has been achieved.

3.4.1.2 Scope

IEC 61508 applies to safety-related systems when one or more of such systems incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices. It covers possible hazards caused by failure of the safety functions to be performed by the E/E/PE safety-related systems, as distinct from hazards arising from the E/E/PE equipment itself (for example electric shock). It is generically based and applicable to all E/E/PE safety-related systems irrespective of the application.

3.4.1.3 Approach

IEC 61508 consists of a series of seven standards4 and:

- uses a risk based approach to determine the safety integrity requirements of E/E/PE safety-related systems, and includes a number of examples of how this can be done;
- uses an overall safety lifecycle model as the technical framework for the activities necessary for ensuring functional safety is achieved by the E/E/PE safety-related systems;
- covers all safety lifecycle activities from initial concept, through hazard analysis and risk assessment, development of the safety requirements, specification, design and implementation, operation and maintenance, and modification, to final decommissioning and/or disposal;

[4] Note that part 0 is a Technical Report, the purpose of which is to introduce the concept of functional safety and to give an overview of the IEC 61508 series of standards.

- encompasses system aspects (comprising all the subsystems carrying out the safety functions, including hardware and software) and failure mechanisms (random hardware and systematic);
- contains both requirements for preventing failures (avoiding the introduction of faults) and requirements for controlling failures (ensuring safety even when faults are present);
- specifies the techniques and measures that are necessary to achieve the required safety integrity.

An example is given below to help give a better understanding of the top level approach:

Consider a machine with a rotating blade that is protected by a hinged solid cover. The blade is accessed for routine cleaning by lifting the cover. The cover is interlocked so that whenever it is lifted an electrical circuit de-energises the motor and applies a brake. In this way, the blade is stopped before it could injure the operator. In order to ensure that safety is achieved, both a hazard analysis and a risk assessment are necessary.

a) The hazard analysis identifies the hazards associated with cleaning the blade. For this machine, it might show that it should not be possible to lift the hinged cover more than 5 mm without the brake activating and stopping the blade. Further analysis could reveal that the time for the blade to stop shall be 1 second or less. Together, these describe the safety function.

b) The risk assessment determines the performance requirements of the safety function. The aim is to ensure that the safety integrity of the safety function is sufficient to ensure that no one is exposed to an unacceptable risk associated with this hazardous event.

The harm resulting from a failure of the safety function could be amputation of the operator's hand or could be just a bruise. The risk also depends on how frequently the cover has to be lifted, which might be many times during daily operation or might be less than once a month. The level of safety integrity required increases with the severity of injury and the frequency of exposure to the hazard.

The safety integrity of the safety function will depend on all the equipment that is necessary for the safety function to be carried out correctly, i.e. the interlock, the associated electrical circuit and the motor and braking system. Both the safety function and its safety integrity specify the required behaviour for the systems as a whole within a particular environment.

To summarise, the hazard analysis identifies what has to be done to avoid the hazardous event, or events, associated with the blade. The risk assessment gives the safety integrity required of the interlocking system for the risk to be acceptable. These two elements, "What safety function has to be performed?" – the safety function requirements – and "What degree of certainty is necessary that the safety function will be carried out?" – the safety integrity requirements – are the foundations of functional safety.

IEC 61508 specifies 4 levels of safety performance for a safety function. These are called safety integrity levels. Safety integrity level 1 (SIL1) is the lowest level of safety integrity and safety integrity level 4 (SIL4) is the highest level. The standard details the requirements necessary to achieve each safety integrity level. These requirements are more rigorous at higher levels of safety integrity in order to achieve the required lower likelihood of dangerous failure.

3.4.2 ISO 26262

3.4.2.1 Introduction

ISO 26262 is the adaptation of IEC 61508 to comply with needs specific to the application sector of electrical and/or electronic (E/E) systems within road vehicles.

With the trend of increasing technological complexity, software content and mechatronic implementation, there are increasing risks from systematic failures and random hardware failures. ISO 26262 includes guidance to avoid these risks by providing appropriate requirements and processes.

System safety is achieved through a number of safety measures, which are implemented in a variety of technologies (e.g. mechanical, hydraulic, pneumatic, electrical, electronic, programmable electronic) and applied at the various levels of the development process. Although ISO 26262 is concerned with functional safety of E/E systems, it provides a framework within which safety-related systems based on other technologies can be considered. ISO 26262:

a) provides an automotive safety lifecycle (management, development, production, operation, service, decommissioning) and supports tailoring the necessary activities during these lifecycle phases;

b) provides an automotive-specific risk-based approach to determine integrity levels [Automotive Safety Integrity Levels (ASIL)];

c) uses ASILs to specify applicable requirements of ISO 26262 so as to avoid unreasonable residual risk;

d) provides requirements for validation and confirmation measures to ensure a sufficient and acceptable level of safety being achieved;

e) provides requirements for relations with suppliers.

3.4.2.2 Scope

ISO 26262 is intended to be applied to safety-related systems that include one or more electrical and/or electronic (E/E) systems and that are installed in series production passenger cars with a maximum gross vehicle mass up to 3,500 kg. ISO 26262 does not address unique E/E systems in special purpose vehicles such as vehicles designed for drivers with disabilities.

ISO 26262 addresses possible hazards caused by **malfunctioning** behaviour of E/E safety-related systems, including interaction of these systems. It does not address hazards related to electric shock, fire, smoke, heat, radiation, toxicity, flammability, reactivity, corrosion, release of energy and similar hazards, unless directly caused by malfunctioning behaviour of E/E safety-related systems.

ISO 26262 **does not address the nominal performance** of E/E systems, even if dedicated functional performance standards exist for these systems (e.g. active and passive safety systems, brake systems, Adaptive Cruise Control).

The two paragraphs above mean that ISO 26262 does not address hazards or risks where the item is intended to contribute directly to their risk reduction. Therefore, it does not cover how these should be assessed, whether the ASIL values reflect the hazard risk or the risk reduction, and (if the ASIL values relate to the hazard risk) how the division of risk mitigation across different items can be accounted for in the safety lifecycles for each of these items.

This is one of the reasons for why the UK committee recorded a negative vote for the acceptance of ISO 26262, part 3. The others included:

- The concept of Automotive Safety Integrity Levels (ASIL) in ISO 26262 is not aligned to the concept of safety integrity level (SIL) found in IEC 61508 and its derivative standards, making application difficult where alignment with these other standards is required.
- IEC 61508 requires risk matrices to be calibrated, but no information on the calibration of the factors for severity, exposure and controllability used in ISO 26262 is provided.

3.4.2.3 Approach

ISO 26262 uses the concept of safety goals and a safety concept as follows:

- a hazard analysis and risk assessment identifies hazards and hazardous events that need to be prevented, mitigated or controlled;
- a safety goal is formulated for each hazardous event;
- an Automotive Safety Integrity Level (ASIL) is associated with each safety goal;

- the functional safety concept is a statement of the functionality to achieve the safety goal(s);
- the technical safety concept is a statement of how this functionality is implemented on the system level by hardware and software; and
- software safety requirements and hardware safety requirements state the specific safety requirements which will be implemented as part of the software and hardware design.

With reference to changes proposed to Regulation 79 proposed in Section 5, in particular for system fault analysis and verification, it is important to evaluate a wide range of failure modes including:

- The impact of a false signal in the hardware if it is propagated into the software.
- The effect of an error in the signal processing algorithm on the hardware.

To this end, it is interesting to note that part four of ISO 26262 provides a reference model for system level design, prescribing that developers carry out both a deductive 'fault tree analysis' (FTA) and an inductive 'fault mode and effects' (FMEA) analysis for systems specified to ASIL levels C and D.

FTA is a top-down methodology in which undesirable behaviours are defined at the top level and then the possible cause(s) outlined. Probabilities are then assigned to each of these types of failure, and combinatory logic used to assess the likelihood and impact of different combinations of failures. Using 'Hardware-in-the-Loop' techniques, the assumptions made in the analysis are evaluated by inserting the different faults into the fault tree to see what happens.

FMEA, on the other hand, is a bottom-up methodology in which possible failures are identified and the effect and propagation of the failure mode determined.

3.4.3 DO-178C

3.4.3.1 Introduction

Since 2003, the European Aviation Safety Agency (EASA) is responsible for the certification of aircraft in the EU (and some European (non-EU countries), e.g. Switzerland). Type-certification consists of the following four stages:

- Technical familarisation and certification basis
  - The aircraft manufacturer presents the project to EASA when it is considered to have reached a sufficient degree of maturity. The EASA certification team and establish the set of rules for certification of the specific aircraft (certification basis).
- Establishment of the certification process
  - EASA and the manufacturer define and agree on the means to demonstrate compliance of the aircraft type for each requirement of the Certification Basis.
- Compliance demonstration
  - The aircraft manufacturer demonstrates compliance of its product with regulatory requirements. This is the longest phase of the type-certification process. In the case of large aircraft, the period to complete the compliance demonstration is set at five years and may be extended, if necessary.
- Technical closure and issue of approval
  - If technically satisfied with the compliance demonstration by the manufacturer, EASA closes the investigation and issues the certificate.

Regulation (EU) 748/2012 Annex I (also referred to as Part 21) and its amendments lay down the implementing rules for the airworthiness and environmental certification of aircraft and related products, as well as certification of design and production organisations. These rules together with related, 'Acceptable Means of Compliance and Guidance Material (AMC/GM) documents', set the basis which can be used by the

manufacturer for the compliance demonstration to obtain certification[5]. Because they are not mandatory, these AMC/GM are often called 'soft-law' (non-binding rules). AMC 20-115C, 'Software consideration for certification of airborne systems and equipment,' sets the basis for software assurance[6]. This AMC recommends the use of the DO-178C standard for software development.

DO-178C provides guidelines that can be followed to provide evidence that software in airborne systems operates consistently with an acceptable level of confidence in safety. DO-178C is a revision of DO-178B and was published in 2011. The document is not mandated by law but represents a consensus of the avionics community in the specification of processes required for an applicant to achieve certification. The European Organisation for Civil Aviation Equipment (EUROCAE), who are the European leader in the development of worldwide industry standards for aviation, helped to develop this standard[7].

D)-178C is separated into several sections, initially describing the system level aspects that must be considered for software development, then moving on to describe the requirements for each stage of the software lifecycle (e.g. activities, objectives, outputs). Additionally, the document discusses the certification and liaison process with an agency.

The document appears to follow a similar safety audit process to ISO 61508. For example, DALs (Design Assurance Levels) are specified for each component depending on the severity of the outcome of an error on the system. However, it could be said that this standard is much more prescriptive in its requirements. One additional feature of this document is that it is stated whether objectives applicable to each Design Assurance Level must be satisfied with independence. In DO-178C, independence is defined as the 'separation of responsibilities which ensures the accomplishment of objective evaluation'.

Independence is achieved differently at each stage of the software lifecycle:

- Planning stage – Each process produces evidence that its outputs can be traced to their activity and inputs, showing the degree of independence of the activity, the environment and the methods to be used.
- Verification independence is achieved when the verification activity is performed by a person(s) other than the developer of the item being verified. A tool may also be used to conduct achieve an equivalent outcome to a human verification activity.
- Quality assurance – Those performing the software quality assurance process must be enabled with the authority, responsibility and independence to ensure that the SQA process objectives are satisfied.

Further associated documents include ARP-4754A (Certification considerations for highly integrated and complex aircraft systems). This is a related standard that provides a development assurance process to reduce the possibility of development errors contributing to aircraft failure conditions. The method was published by SAE (Society of Automotive Engineers).

[5] Easy Access Rules for Initial Airworthiness: AIRWORTHINESS AND ENVIRONMENTAL CERTIFICATION: Consolidated version of Part-21 Implementing Rules and related Acceptable Means of Compliance and Guidance Material; https://www.easa.europa.eu/document-library/technical-publications/easy-access-rules-initial-airworthiness

[6] AMC 20-115C – Software consideration for certification of airborne systems and equipment https://www.easa.europa.eu/system/files/dfu/Change%20Information%20Amdt%2010.pdf

[7] http://www.eurocae.net/

3.4.3.2 Scope

DO-178C applies to the production and certification of software for avionic systems and equipment used of aircraft (e.g. engines, propellers, auxiliary power unit etc.). The document discusses the software life cycle and specifies activities necessary for certification to show that airworthiness requirements are fulfilled.

3.4.3.3 Approach

The document is split into sections covering the software lifecycle processes including: planning, development (requirements, design, coding and integration), integral (verification, configuration, quality assurance) and the certification processes.

For each section, a number of objectives are defined with their applicability by design assurance level stated, alongside an indicator to show whether an objective must be satisfied with independence. Activities (e.g. define development standards) and outputs (e.g. plan for software aspect of certification) required to fulfil the safety requirements of each objective are listed. Finally, the control category by software level is also defined.

The design assurance level for each component is determined by the safety audit process. The level is awarded based on the effect of a failure of the component.

A – Catastrophic – safety of the flight is compromised

B – Hazardous – serious damage and fatalities

C – Major – dysfunction of vital equipment of the unit

D – Minor – safety incident that can be contained by the crew

E – No effect – no effect over flight safety (no objectives).

The allocated DAL is linked to a set of processes to follow when developing the system – the higher the level then the more rigorous and stringent these processes are. As an example, let's consider code coverage requirements. The purpose of code coverage testing is to determine how much of the code has been exercised by the requirements based test cases. It is a powerful tool to locate any code that doesn't trace to a requirement, or limitations in verification testing. The more severe the consequences of the code going wrong, then the more evidence needed that the test cases can find potential problems in the code.

Table 5 shows the code coverage requirements for DO178C from Annex A, Table A-7 of the standard. At Level C you only need to demonstrate that your tests cover all the statements in your software. However, at Level A you need three types of code coverage, including the most stringent, Multiple Condition/Decision Coverage for which every possible condition must be shown to independently affect the decision/software's outcome. Furthermore, you need to run these tests and demonstrate that the testing process has been performed by someone not directly involved with the development process.

Table 5: Code coverage requirements in DO-178C

	MC/DC	Decision Coverage	Statement Coverage
Level A	With Independence	With Independence	With Independence
Level B		With Independence	With Independence
Level C			Required
Level D			
Level E			

In contrast the code coverage requirements are quite different. Table 6 shows the requirements from Tables 12 and 15 of Part 6 of ISO 26262. There are two different sets, one at the unit level and one at the architectural level. Techniques are highly recommended (++) or recommended (+). There is no requirement for independence. So

whilst at the highest ASIL, Multiple Condition/Decision Coverage (MC/DC) are required as with DO178C, the requirement for how this is achieved is different. Also code coverage must be applied at multiple abstraction levels.

Table 6: Code coverage requirements in ISO 26262

	MC/DC (Unit coverage)	Branch coverage (Unit level)	Statement coverage (Unit level)	Functional coverage (Architectural level)	Call coverage (Architectural level)
ASIL D	++	++	+	++	++
ASIL C	+	++	+	++	++
ASIL B	+	++	++	+	+
ASIL A	+	+	++	+	+

3.4.4 Summary / conclusions

- The main standard for safety related systems which incorporate electrical and/or electronic and/or programmable electronic (E/E/PE) devices is IEC 61508. This standard is generically based and applicable to all E/E/PE safety-related systems irrespective of the application. Functional safety standards in most industries (e.g. railway, nuclear, automotive), with the exception of the avionics industry, have been derived from IEC 61508, e.g. automotive ISO 26262.
- For the automotive industry, ISO 26262 addresses possible hazards caused by **malfunctioning** behaviour of E/E safety-related systems, including interaction of these systems. However, it does not address the **nominal performance** of E/E systems.
- DO-178C (Certification standard for avionics) is similar in concept to ISO 26262 in that both sets of standards use integrity levels, Design Assurance Levels (DALs) and (Automotive) Safety Integrity Levels (ASILs), respectively. However, the requirements of these levels are quite different in terms of the scales and criteria used.

3.5 Verification Methods

Verification methods are applied differently depending on the software development cycle process followed. For example, the V-cycle software development model, which is commonly followed in the automotive industry and is part of the ISO 26262 requirements, allows work to be defined in separate stages, meaning that different teams can work in parallel while defining project requirements (falling edges) and developing test and verification requirements (rising edges). This means that verification activities can be planned and executed earlier in the development phase, leading to greater efficiency through time saving and the identification of problems earlier.

Verification methods may include:

- Inspections – Systematic and formal peer review following a defined procedure. Reviews may focus on removing defects and improving the process.
- Informal reviews – These reviews may be spontaneously held at a developer's desk or could occur over email if flexibility is required.
- Walkthrough reviews – Informal review where the code author presents their code in a meeting to their peers. Meeting participants may then provide feedback if defects, security or safety problems are identified.
- Plastic duck method – A developer may identify weaknesses or incorrect technical choices in their code by pretending to explain the methodology to a plastic duck.

- Pair programming – An Agile technique where two developers work together to create one piece of code. One developer writes the code while the other observes and checks each line. The roles are exchanged regularly.
- Refactoring - Continuously reworking a line of code to increase its simplicity, efficiency and readability to ensure that multiple contributions to the source code do not degrade the quality.
- Test-driven development – The practice of defining tests before the code is written to ensure that code will meet all required specifications.
- Feature-driven development – Iterative method consisting of five activities: definition of overall model, production of list of features, project planning, design by feature (production of design packages after design features are implemented and validated), build by feature (packages are grouped to provide functions for the end user).
- Behaviour-driven development – Focussed on value for the customer and encourages communication between all stakeholders involved in software project. BDD uses neutral language to describe the purpose of the source code and remove language barriers between customers, users and developers (e.g. 'I need <goal> so that <benefit> becomes 'In this scenario, when <event occurs> ensure <beneficial outcome>.

3.6 Other literature

This section contains useful supplementary background information related to the development of standards for the assessment of complex automated systems within the automotive industry. The results of some relevant projects supported by the EC and NHTSA are described.

3.6.1 European Commission projects

3.6.1.1 ADAS CoP developed by RESPONSE

Within the EC PREVENT integrated project there was a series of three subprojects called RESPONSE. One of the key deliverables from this series of subprojects, which started in 1998 and finished in 2006, was a Code-of-Practice (CoP) for engineers involved in the development of Advanced Driver Assistance Systems (ADAS) (Response-3, 2009).

Driver Assistance Systems support the driver in the primary driving task. They inform and warn the driver, provide feed-back on driver actions, increase comfort and reduce the workload by actively stabilising or manoeuvring the car. However, they do not take over the driving task completely, thus the responsibility always remains with the driver.

ADAS were defined as a subset of driver assistance systems having **all** the following properties:

- support the driver in the primary driving task
- provide active support for lateral and/or longitudinal control with or without warnings
- detect and evaluate the vehicle environment
- use complex signal processing
- direct interaction between the driver and the system

The aim of the CoP was to provide a support tool for engineers that gave some guidance to help them determine activities required during the development phases of ADAS and also contained a compilation of relevant procedures currently available (at that time). The focus of the CoP was the design of the system in terms of controllability and the Human Machine Interaction (HMI). This included the influence of system defects / errors, the ADAS behaviour at system limits and foreseeable misuse.

Controllability refers to the entire ADAS-driver-environment interaction comprising:

- normal system use within system limits,
- usage at and beyond exceeding system limits and

- usage during and after system failures.

Controllability is dependent upon:

- the possibility and driver's capability, to perceive the criticality of a situation,
- the drivers capability to decide on appropriate countermeasures (e.g. override, system switch-off) and
- the driver's ability to perform the chosen countermeasure (e.g. reaction time, sensory-motor speed, accuracy).

Safe use of a system requires controllability, and hence controllability is one of, or possibly, the most important design requirement. On this basis, the CoP contains detailed recommendations of how to verify controllability and that the driver can and will react in an expected an appropriate way:

- Final proof of controllability by an interdisciplinary expert panel
- Final proof of controllability by a test with 'naïve' subjects (i.e. non expert drivers)
- Final proof by direct recommendation of controllability sign-off by the ADAS development team

It is interesting to note that ISO 26262 was under development at the time this CoP was published and that controllability was included as a fundamental parameter within the ISO 26262 hazard analysis and risk assessment. It is clear that it should also be a key part of any safety assessment of ADAS type systems for the future.

3.6.1.2 ADAPTIVE

Adaptive is a current EC 7th framework project which started 1st January 2014 and is scheduled to complete 30th June 2017 (Adaptive, 2016). Its main objective is to develop automated driving functions for daily traffic by dynamically adapting the level of automation to situation and driver status. Demonstrators will be built. As part of the work to do this Adaptive will:

- Expand the range of possible situations for the application of automated driving
  - Focus on supervised automated driving in highway scenarios, urban traffic and close distance manoeuvres
- Enhance perception and communication capabilities
  - Implement features concerning the sensor platform, communication with other vehicles or with nearby infrastructure
  - Improve safety in potentially dangerous situations via cooperative manoeuvres
- Develop solutions for cooperative control addressing driver needs
  - Ensure continuous interaction between human and automation
  - Create and evaluate guidelines for implementation
- Design and demonstrate resilient behaviour for the applications
  - Develop fail-safe architecture and an automated function to bring the vehicle to a halt
  - Implement support functions according to the infrastructure and driver capabilities
- Improve the safety and adaptability of automated driving
  - Integrate solutions for driver-status monitoring
- Develop and apply specific evaluation methods
  - Develop new methods for the technical and user-related assessments
  - Generate new methods to analyse safety and environment impacts at the European level
- Analyse legal aspects
  - Examine legal conditions and identify possible barriers for the market introduction of partially and highly automated systems
  - Establish requirements for safety validation and specify qualifications for system availability

Many project deliverables are not available yet, as the project is still ongoing. However, the following project outputs located on the project website (Adaptive, 2016) contained relevant information:

- D2.1 'System classification and glossary'.
  - Presents an approach for the classification of automated driving and parking functionalities and gives examples for different automation levels.
- Athens conference April 2016, 'Experiences with automated driving functionalities in heavy duty vehicles – driver is allowed to do secondary tasks'.
  - Presents concept of allowing driver to perform secondary tasks whilst using traffic jam pilot. However, recommended that to ensure safety driver should be able to take over driving task within 10 sec.
- Athens conference April 2016, 'Regulatory update: EU member states and beyond'.
  - Presents useful overview of current automated and connected driving research activities in the EU.

3.6.2 NHTSA's Electronics Reliability Research

As part of NHTSA's automotive electronics reliability research programme, Volpe has performed a study that assessed and compared six industry and government safety standards relevant to the safety and reliability of automotive electronic control systems (Van Eikema Hommes, 2016). The standards were:

- ISO 26262: Road Vehicles - Functional Safety
  - ISO 26262 is the first comprehensive automotive safety standard that addresses the functional safety of the growing number of E/E and software-intensive features in today's road vehicles. It is an adaptation of IEC 61508.
- MIL-STD-882E: Department of Defence Standard Practice - System Safety
  - MIL-STD-882E is the U.S. Department of Defence Systems Engineering approach for eliminating hazards, where possible, and minimizing risks where those hazards cannot be eliminated.
- DO-178C: Software Considerations in Airborne Systems and Equipment Certification
  - DO-178C is an industry-accepted guidance for software in airborne systems and equipment in the Aviation industry.
- FMVSS: Federal Motor Vehicle Safety Standard
  - Motor vehicle safety in an FMVSS considers the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident. Motor vehicle safety also includes the non-operational safety of a motor vehicle.
- AUTOSAR: Automotive Open System Architecture
  - The AUTOSAR standard consists of a set of specifications that describe a software architecture, application interfaces and a methodology. The AUTOSAR layered software architecture enables the development of independent software components. These can be used in vehicles of different manufacturers, and in electronic components of different suppliers that can span multiple product generations. It results in a high reliability of the overall system with significant cost and capacity benefits.
- MISRA C: Guidelines for the Use of the C Language in Critical Systems
  - MISRA C is a standard concerning the use of C language in safety-related automotive embedded systems. The C language is heavily used in the development of safety-critical software where reliability is a prime concern. ISO 26262 recommends following MISRA C for software coding.

The standards were compared on the basis of the following eleven criteria:

1. Type of standard
2. Definition of safety and hazard
3. Identification of safety requirements
4. Hazard and safety analysis methods

5. Management of safety requirements
6. Risk assessment approach
7. Design for safety approach
8. Software safety
9. System lifecycle consideration
10. Human factors consideration
11. Approach to review, audit, and certification

Related to approaches for the assessment of functional safety, the following observations were made:

- Process safety standards that follow a systems engineering approach are different than FMVSSs and complement existing standards for safety assurance.
- Existing process standards could be enhanced by providing a precise definition of "unreasonable risk" within the context of automotive safety.
- Hazard definitions vary across different standards.
- Severity alone can be used as the risk measure for software, similar to the approach outlined in DO-178C. Further, in cases when statistically valid failure probability or the probability of the occurrence of a mishap is not available, severity could be used as the only measure.
- Exposure and controllability assessment used by the industry, as defined in the ISO 26262 standard, could be enhanced with the collection of additional data through design of specific experiments.
- Existing process standards for software design could be enhanced with consideration for the overall safety of the control systems and software safety certification, in addition to the focus on specific aspects of the design solution (i.e., good architecture and coding standard).
- Design-for-safety approach as specified in MIL-STD-882E provides a framework that could be leveraged for separate management of hazard tracking/safety requirements from regular system requirements, simpler risk assessment, and more emphasis on human factors.
- The topic of health hazard analysis for drivers and service technicians could be further assessed for the appropriateness of including this topic in a process standard.
- Existing process standards do not explicitly address environmental impacts on a vehicle throughout its lifecycle, including testing, manufacturing, operation, maintenance, etc.
- Human factors studies could be better integrated into a comprehensive functional safety approach.

3.7 Summary and conclusions

The review of safety testing processes in other industries (railway, nuclear, process and machine) found that the main standards were, in principle, similar to the automotive industry, mainly because they were all derived from IEC 61508 which sets out a generic approach for electrical/electronic/programmable electronic systems used to perform safety functions. The generic approach consists of the following:

- Hazard identification and risk assessment
- Setting of safety requirements (goals)
- Verification of safety requirements

The main standard for the aviation industry, namely DO-178C, was not derived from IEC 61508. Even so, its approach is often similar, for example, for safety requirements and their verification both IEC 61508 and DO-178C use the concept of Safety Integrity Levels (SILs) although DO-178C calls them Design Assurance Levels (DALs). However, DO-178C does not contain guidance for identification of safety hazards; in DO-178C hazards are considered to be caused by software behaviour inconsistent with specified requirements.

From a point of view of assuring the safety of electrical/electronic/programmable electronic systems, the review above clearly shows that an assessment of the development life cycle (including processes and standards followed and verification of safety requirements (goals)) is needed as part of the regulatory requirements,.

Key aspects of a regulatory assessment should include:

- Hazard identification and risk assessment with focus on controllability and consideration of human factors in particular the Human Machine Interface (HMI)
- Management of safety requirements in particular verification of them.

It is interesting to note that, from a regulatory point of view, the certification process of aircraft is similar to that for cars in that they both use a type-approval (certification) process. However, there are some notable differences:

- For aircraft the process is defined in much greater detail by direct reference to the use of certain standards in 'Acceptable means for compliance (AMC)' documents. For software development AMC 20-115C recommends directly the use of DO-178C. In contrast for automobiles no direct recommendations for use of specific standards are made for software development, although ISO 26262 appears to be becoming the norm.

For aircraft the process often takes much longer; compliance demonstration may be greater than five years for large aircraft; for automobiles it is usually much less than a year.

4 Task 3: Review current ACSF IWG proposal

4.1 Introduction

The objective of this task was to review the current ACSF IWG proposal (Informal documents: ACSF-06-28 and ACSF-07-20), identify any potentially safety-relevant issues or omissions and make initial recommendations of how they may be resolved. The focus was to ensure safe system function in all real-world driving situations.

The section below summarises the categories of corrective steering functions (CSF) and automatically commended steering functions (ACSF). The following sections review the proposed requirements for each CSF and ACSF steering category and provide initial recommendations and the final section summarises the main issues identified.

4.2 System categories

UN Regulation 79 separates steering functions into two main groups: Corrective steering functions (CSF) and automatically commanded steering functions (ACSF). The current draft amendments separate ACSF further into six distinct categories: A, B1, B2, C, D, E. The classification is based on the functional intent (low-speed manoeuvring, lane keeping, or lane changing) and the system capabilities, i.e. the level of input and monitoring required from the driver (hands-on or hands-off system). The system category determines the applicable requirements and test procedures.

The latest working group drafts define the categories as follows:

CSF:

> *"Corrective steering function (CSF)" means a control function within an electronic control system whereby, for a limited duration [and independent of the drivers demand] changes to the steering angle of one or more wheels may result from the automatic evaluation of signals initiated on-board the vehicle, in order to assist the avoidance of a collision, or to compensate a sudden, unexpected change in the sideforce to improve the vehicle stability (e.g. sidewind, µ-split) or to correct lane departure after crossing the lane marking."* (ACSF–07-20)

ACSF general:

> *""Automatically commanded steering function" (ACSF) means the function within a complex electronic control system where actuation of the steering system can result from automatic evaluation of signals initiated on-board the vehicle, possibly in conjunction with passive infrastructure features, to generate continuous control action in order to assist the driver."* (ACSF–06-28)

ACSF Category A (Low-speed systems):

> *"Category A ACSF means, a function that operates at a speed no greater than 10 km/h to assist the driver, on demand, in low speed lateral manoeuvring or lateral parking operations."* (ACSF–06-28)

ACSF Category B1 (Hands-on lane keep assistance systems):

> *"ACSF Category B1 means a function [which is initiated/activated by the driver and] which continuously assists the driver in keeping the vehicle within the chosen lane, by influencing the lateral movement of the vehicle."* (ACSF–06-28)

ACSF Category B2 (Hands-off lane guidance systems):

> *"ACSF Category B2 means a function which is initiated/activated by the driver and which keeps the vehicle within its lane by influencing the lateral movement of the*

vehicle for extended periods without further driver command/confirmation" (ACSF–06-28)

ACSF Category C (Lane change systems on driver command):

"Category C ACSF means, a function which is initiated/activated by the driver and which can perform a single lateral manoeuver (e.g. lane change) when commanded by the driver." (ACSF–06-28)

ACSF Category D (Lane change systems on driver confirmation):

"Category D ACSF means, a function which is initiated/activated by the driver and which can indicate the possibility of a single lateral manoeuvre (e.g. lane change) but performs that function only following a confirmation by the driver." (ACSF–06-28)

ACSF Category E (Lane change systems without driver input):

"Category E ACSF means, a function which is [initiated/activated] by the driver and which can continuously determine the possibility of a manoeuvre (e.g. lane change) and complete these manoeuvers for extended periods without further driver command/confirmation." (ACSF–06-28)

4.3 Review of proposed requirements and tests

The contents of the latest draft proposal/working document for each system category are analysed in the following sections. The tables summarise the most important aspects of the proposed requirements and test procedures and provide a brief commentary and recommendation (bold text) where TRL identified potential issues or gaps.

To provide a structured overview that allows assessing the completeness of a proposal, the prescriptions are organised into the following categories:

- Safety under normal operating conditions
- Safety under fault conditions
- Driver monitoring / system misuse
- Driver information
- Transition demand and related safety manoeuvres
- Incidents

Major issues identified are noted briefly in the tables and discussed further in more detail in Section 4.4.

4.3.1 CSF

The latest available draft requirements for CSF systems are contained in the report of the 7th meeting (ACSF-07-20).

Table 7: Review of proposed requirements and tests for CSF systems

System category: CSF	
Safety under normal operating conditions	
Functional safety	Annex 6: CEL audit as required for all complex electronic systems. The interpretation and application of this Annex might be inconsistent between different technical services. **Recommend to amend Annex 6 to ensure current best practice is applied consistently. See Section 4.4.1.**
Safety under fault conditions	

Functional safety	Annex 6: CEL audit as required for all complex electronic systems. **See comment above (Safety under normal operating conditions – Functional safety)**
Driver monitoring / system misuse	
Driver monitoring/ misuse prevention	No requirements in current draft except for the signal cascade described below (Driver information – System status indication). **No recommendations**
Driver information	
System status indication	Agreement was reached that the driver should be informed of any intervention by a CSF. No details agreed yet on how to define this. For interventions to correct a lane departure, a cascade of optical and audible signals was specified in ACSF-07-20, Section 6.2.2. Note that audible warnings are only required for more extreme cases of lane departure intervention to ensure CSF not too annoying for driver, namely: • "*In the case of a lane departure intervention longer than [30s], an acoustic warning shall be provided until the end of the intervention*" • "*In the case of 2 or more consecutive lane departure interventions within a rolling interval of 180s and in the absence of a steering input by the driver during the intervention, an acoustic warning shall be provided by the system during the second and any further intervention*". **Recommend to define a test to verify this requirement**
Transition demand and related safety manoeuvres	
	Not applicable to CSF
Incidents	
	Not applicable to CSF

4.3.2 ACSF Category A

The latest working documents discussed by the working group (ACSF-06-28, ACSF-07-20) do not contain any requirements or test procedures for Category A systems yet.

4.3.3 ACSF Category B1

The latest available draft requirements and tests for Category B1 systems are distributed across different documents:

- ACSF-07-02 (Proposal by Contracting Parties for requirements based on ACSF-06-28)
- ACSF-07-13 (Proposal by industry based on ACSF-07-02)
- ACSF-07-20, Sections 6.3., 6.4. and 6.5. (Report of 7th meeting)

No agreement has been reached by the group yet on the full suite of requirements and tests. The following review focusses on the latest draft discussed regarding each aspect, i.e. mainly ACSF-07-20.

Table 8: Review of proposed requirements and tests for ACSF Category B1

System category: ACSF Category B1	
Safety under normal operating conditions	
Operating conditions / capabilities	5.6.5.1.1. refers to 'boundary conditions' under which the system shall prevent lane crossing. Currently defined as a general provision and not clear whether these are OEM-defined or regulator-defined. **Recommend to expressly define these boundary conditions in the regulation to ensure equal minimum performance across the field. Might define factors such as: Road curvature, camber angles, surface conditions wet/dry, etc. Should consider technical capabilities of current systems, likely customer expectations and road design standards (what is to be expected in the field).**
Controllability	5.6.5.1.3. requires that excessive steering interventions shall be prevented. Currently defined as a general provision. **Recommend to specify this paragraph in more detail. What is 'excessive intervention'? Potentially base on ISO 11270, Section 5.4 (this defines maximum lateral acceleration, lateral jerk, longitudinal acceleration, longitudinal speed deceleration, fading out intervention).**
Driver override	5.6.5.1.3. in ACSF-07-13 defines maximum necessary control effort to override the system; this paragraph is not included in ACSF-07-20 although values were discussed during the 7th meeting. **Recommend to re-introduce the sentence from ACSF-07-13 and define suitable limit values, which should be considerably lower than those for failing steering equipment.**
Tests	Annex 7: FU0 test. Test for lane keeping and holding steering control. **Recommend to separate into two tests for clarity: (A) a lane-keep performance test and (B) a hands-off warning and deactivation test. Recommend to define (A) in more detail than the current draft (departure rate, curvature). Potentially base on ISO 11270, Section 6.5.2 and/or 6.5.3. Alternatively, if clear 'boundary conditions' are specified in regulation, this could be changed to a challenging worst case test.** **Recommend to make (B) a worst case test for hands-off detection. The case most difficult to detect for torque-measuring systems is allegedly at low driving speed on a straight, smooth road, because the driver input is minimal.**
Safety under fault conditions	
Functional safety	Annex 6: CEL audit as required for all complex electronic systems. The interpretation and application of this Annex might be inconsistent between different technical services. **Recommend to amend Annex 6 to ensure current best practice is applied consistently. See Section 4.4.1.**
Driver monitoring / system misuse	
Driver monitoring/ misuse prevention	5.6.5.2.4: Hands-off detection (steering wheel) with warning after [30 seconds] and system deactivation after another [30 seconds]. **Recommend to create evidence base or clear rationale to define these timescales. The representatives of South Korea and OICA agreed to review this.** **Recommend to consider whether deactivating the system is a sufficiently safe state or if this introduces a hazard. Could a loud audible signal, for example, be similarly effective at misuse prevention?**

System category: ACSF Category B1	
Tests	Annex 7: FU0 test. Test for lane keeping and holding steering control. **See comments above (Safety under normal operating conditions – Tests)**
Driver information	
System status indication	5.6.5.2 requires optical signal for: System active, System not available (e.g. inclement weather); and a signal of choice for: System failure. **No recommendation**
Transition demand and related safety manoeuvres	
	Not applicable to ACSF Category B1 (hands-on system)
Incidents	
	Not applicable to ACSF Category B1 (hands-on system)

4.3.4 ACSF Category B2

The latest draft of requirements for ACSF Category B2 is contained in the working document after the 6th session (ACSF-06-28). The contents are largely a copy of the text for Category E (albeit reflecting the status before the changes made for Category E during the 6th session). Considering that Category B2 and Category E both describe "hands-off" systems it is reasonable to define closely aligned requirements for all aspects except the core functionality (where the requirements will be different between the lane keeping and the lane changing function). Therefore, where the review comments for Category B2 are identical to those for Category E, the table below makes reference to the Category E review rather than repeating the comments in full.

Table 9: Review of proposed requirements and tests for ACSF Category B2

System category: ACSF Category B2	
Safety under normal operating conditions	
Operating conditions / capabilities	5.6.4.1.1. to 5.6.4.1.6. requires the following operating conditions: Deliberate activation by driver to enable operation of ACSF, all associated functions working correctly, vehicle speed less than 130 km/h, vehicle lateral acceleration less than 3 m/s^2 (or 1 m/s^2 at high speeds; reference currently missing in document). **No recommendations** 5.6.4.2.2. contains the requirements defining the system functionality: "*shall at any time ensure that the vehicle does not cross any lane marking".* This description is unspecific and does not describe the intended function in a suitable form (the vehicle will under certain circumstances cross lane markings). In its current form this requirement cannot be verified, i.e. it has no acceptance criteria. **Recommend:** • **to adapt wording to only prevent <u>unintended</u> crossing of lane marking within specified boundary conditions.** • **to define boundary conditions for prevention of unintended crossing of lane marking. This could be tied into the FU1 test case provided it is a 'worst test' case – see comments on tests in rows below.**
Monitoring ranges	See corresponding comments regarding ACSF Category E (Table 11).

System category: ACSF Category B2	
Driver override	5.6.2.1.3. defines driver override by any steering intervention, but does not define the force/torque the driver has to exert to override. **Recommend to introduce suitable limit values for the maximum necessary steering effort by the driver to override the system (to ensure that the override can be performed easily by all drivers), which should be considerably lower than those for failing steering equipment.**
Tests	Annex 7 currently defines 10 tests, of which 3 are related to safety under normal operating conditions ('functionality tests'): FU1, FU2 and FU3. FU1 (lane keeping) is the only functionality test required for Category B2 systems. FU2 and FU3 are related to lane changing. **Recommend to define FU1 in more detail than current draft to ensure a worst case test when clear 'boundary conditions' are defined.** **Recommend to verify whether existing test tracks could accommodate the test FU1 as currently prescribed with regard to length of available straight and curved sections.** While this test can help to demonstrate the performance of the system to the technical service, it will not be possible to capture the large variety of scenarios, configurations and environmental conditions encountered in the real-world with a limited number of test setups. The conventional approach of relying on a 'worst case' test is also not feasible with complex software algorithms, where this worst case cannot be defined. **Recommend to define additional validation requirements to ensure safety operations under all real-world conditions (Annex 'x'). See Section 4.4.2.**
Safety under fault conditions	
Sensor failures	See corresponding comments regarding ACSF Category E (Table 11).
Functional safety	Annex 6: Complex Electronic (CEL) system audit as required for all CEL systems. The interpretation and application of this Annex might be inconsistent between different technical services. **Recommend to amend Annex 6 to ensure current best practice is applied consistently. See Section 4.4.1.**
Driver monitoring / system misuse	
Driver monitoring/ misuse prevention	See corresponding comments regarding ACSF Category E (Table 11).
Road type limitation	See corresponding comments regarding ACSF Category E (Table 11).
Driver responsibilities	See corresponding comments regarding ACSF Category E (Table 11).
Vehicle owner information	See corresponding comments regarding ACSF Category E (Table 11).
System status indication	See corresponding comments regarding ACSF Category E (Table 11).
Tests	See corresponding comments regarding ACSF Category E (Table 11).
Transition demand and related safety manoeuvres	
Transition demand (TD)	See corresponding comments regarding ACSF Category E (Table 11).
Minimal risk manoeuvre (MRM)	See corresponding comments regarding ACSF Category E (Table 11).

System category: ACSF Category B2	
Emergency manoeuvre (EM)	See corresponding comments regarding ACSF Category E (Table 11).
Tests	See corresponding comments regarding ACSF Category E (Table 11).
Incidents	
Incident recording (DSSA)	See corresponding comments regarding ACSF Category E (Table 11).

4.3.5 ACSF Category C

The latest available draft requirements and test procedures for Category C systems are contained in the consolidated working document after the 6th meeting (ACSF-06-28).

Table 10: Review of proposed requirements and tests for ACSF Category C

System category: ACSF Category C	
Safety under normal operating conditions	
Operating conditions / capabilities	5.6.3.3.1.1. states that boundary operating conditions (minimum and maximum speed, lateral acceleration) are OEM-defined rather than regulator-defined. (5.6.3.1.4. specifies a maximum cap for the lateral acceleration.) **Recommend to consider adding an upper limit for the OEM-defined maximum speed as currently done for Category D and E. It should be investigated whether using Category C systems at high speeds might create safety hazards.** 5.6.3.2.4. requires lane keeping functionality. According to the definitions, Category C is a lane change system; all lane keeping functions are organised under Categories B1 and B2 and not relevant for Category C. **Recommend to remove the lane keeping requirement and define in another part of the regulation what combinations of systems are permissible (require B1 or B2 in combination with C).**
Controllability	5.6.3.1.4. specifies a range for the maximum acceleration which is related to lane keeping, but not lane changing. **Recommend to remove the lane keeping requirement and define in another part of the regulation what combinations of systems are permissible (require B1 or B2 in combination with C).** There are no provisions against excessive steering interventions. **Recommend to consider specifying provisions to prevent excessive steering interventions such as maximum lateral jerk to ensure controllability of the car during a lane change manoeuvre.**
Driver override	5.6.3.1.3. defines driver override by any steering or brake intervention, but does not define the force/torque the driver has to exert to override. **Recommend to introduce suitable limit values for the maximum necessary steering effort by the driver to override the system (to ensure that the override can be performed easily by all drivers), which should be considerably lower than those for failing steering equipment.**

System category: ACSF Category C	
Tests	5.6.3.1.7. requires lane keep test (FU1) and lane change test (FU3). **Recommend to remove the requirement for a lane keep test. See comments under Safety under normal operating conditions – Operating conditions / capabilities.** **Recommend to adapt the definition of Annex 7, Test FU3, which is currently not suitable for a Category C system (because it does not automatically decide to perform a lane change and does not necessarily automatically adjust speed and does not necessarily move back to the initial lane after completion).**
Safety under fault conditions	
Functional safety	Annex 6: Complex electronic (CEL) system audit as required for all complex CEL systems. The interpretation and application of this Annex might be inconsistent between different technical services. **Recommend to amend Annex 6 to ensure current best practice is applied consistently. See Section 4.4.1.**
Driver monitoring / system misuse	
Driver monitoring/ misuse prevention	5.6.3.2.3. requires that lane changes are not performed if system detects an "*imminent critical situation*". This requirement is unspecific and the intention unclear. **Recommend to investigate whether category C systems without lane change abort could create a safety hazard if people overestimate the system capabilities. Based on the outcome recommend to define clearly whether and in what scenarios (vehicle adjacent lane occupied, fast approaching vehicle from behind, etc.) Category C systems shall ensure lane change abort functionality. Driver misinterpretation of functionality between Categories C, D and E could be a major safety issue.**
Road type limitation	The draft currently does not contain any requirements to limit this system to certain road types, e.g. those where no oncoming traffic is to be expected. This could prevent users from misinterpreting the system capabilities and using it for overtaking on single carriageway roads with oncoming traffic. **Consider adding a requirement, and potentially test, to restrict system activation to suitable road types, e.g. dual carriageways (geo-fencing).**
Tests	The draft currently does not require a lane change abort test. **Recommend to define and require an appropriate lane change abort test, if this functionality is required for Category C (see comments above under Driver monitoring / system misuse – Driver monitoring/ misuse prevention). This could be based on a modification of the definition of Annex 7, Test FU2, which is currently not suitable for a Category C system (because it does not automatically decide to perform a lane change and does not necessarily automatically adjust speed).**
Driver information	
System status indication	5.6.3.1.6. requires optical signal for stand-by, active and failure. **No recommendation**
Transition demand and related safety manoeuvres	
	Not applicable to ACSF Category C (hands-on/driver commanded system)
Incidents	
	Not applicable to ACSF Category C (hands-on/driver commanded system)

4.3.6 ACSF Category D

The latest available draft requirements and test procedures for Category D systems are contained in the consolidated working document after the 6th meeting (ACSF-06-28). These requirements are broadly identical to the requirements proposed for Category E (albeit reflecting the status before the changes made for Category E during the 6th session), which are reviewed in Section 4.3.7. The comments provided are also applicable to Category D but not repeated here to avoid duplication.

The only major difference in the current draft requirements is that a data storage system for ACSF (DSSA) is not required for Category D. This EDR-type functionality would be beneficial for collision investigations (criminal and civil) of automated driving systems of all levels, but will be vital at least for systems that initiate a lane change autonomously. Because Category D systems perform a lane change only after a positive action of the driver (confirmation) it might be justified to not impose this requirement on Category D.

4.3.7 ACSF Category E

The latest available draft requirements and test procedures for Category E systems are contained in the consolidated working document after the 6th meeting (ACSF-06-28).

Table 11: Review of proposed requirements and tests for ACSF Category E

System category: ACSF Category E	
Safety under normal operating conditions	
Operating conditions / capabilities	5.6.1.1.1. to 5.6.1.1.6. requires the following operating conditions: Deliberate activation by driver to enable operation of ACSF, all associated functions working correctly, vehicle speed less than 130 km/h, vehicle lateral acceleration less than 3 m/s^2 (or 1 m/s^2 at high speeds). **No recommendations** 5.6.1.2.4. requires lane keeping functionality. According to the definitions, Category E is a lane change system; all lane keeping functions are organised under Categories B1 and B2 and not relevant for Category E. **Recommend to remove the lane keeping requirement and define in another part of the regulation what combinations of systems are permissible (require B2 in combination with E).**
Monitoring ranges	5.6.1.1.8. defines minimum monitoring ranges for front, rear and side detection. Not clearly defined under what environmental conditions these minimum ranges need to be achieved and what type of vehicles needs to be detected. No test is defined to verify this requirement. 5.6.1.1.8.1. (Front): Currently ca. 176 metres required. This is based on the braking distance in wet conditions. 5.6.1.1.8.2. (Rear): Currently based on an assumed speed of approaching vehicle of 130 km/h. This value might need to be increased considering other drivers speeding, police cars and high speed vehicles on unrestricted German motorways. 5.6.1.1.8.3. (Side): Currently 7 metres. More would be required to detect with certainty vehicles two lanes over (which might merge to centre lane). **Recommend to either:** • **remove fixed requirements for monitoring ranges and define a more performance-based specification; or** • **specify the requirements in more detail (what size and type of object needs to be detected in these ranges; under what environmental conditions; is the object to be detected moving against the background; etc.) and define suitable test procedures.**

System category: ACSF Category E	
Driver override	5.6.1.1.3. defines driver override by any deliberate steering or brake intervention, but does not define the force/torque the driver has to exert to override. Note that 5.6.1.2.3. only refers to steering as an action to override the system (not braking). **Recommend to introduce suitable limit values for the maximum necessary steering effort by the driver to override the system (to ensure that the override can be performed easily by all drivers), which should be considerably lower than those for failing steering equipment.**
Tests	Annex 7 currently defines 10 tests, of which 3 are related to safety under normal operating conditions ('functionality tests'): FU1, FU2 and FU3. FU1 is related to lane keeping functionality, not lane changing. **Recommend to remove the requirement for this test for Category C (and rather cover it under Category B2). See comments under Safety under normal operating conditions – Operating conditions / capabilities.** **Recommend to verify whether existing test tracks could accommodate the tests FU2 and FU3 as currently prescribed with regard to length of available straight and curved sections.** While these tests can help to demonstrate the performance of the system to the technical service, it will not be possible to capture the large variety of scenarios, configurations and environmental conditions encountered in the real-world with a limited number of test setups. The conventional approach of relying on a 'worst case' test is also not feasible with complex software algorithms, where this worst case cannot be defined. **Recommend to define additional validation requirements to ensure safety operations under all real-world conditions (Annex 'x'). See Section 4.4.2.**
Safety under fault conditions	
Sensor failures	5.6.1.4.2.3.: for a single sensor failure the system shall be able to follow the desired path for at least 4 seconds. 5.6.1.4.5.: for other failures transition demand given immediately and fail-safe strategy as declared by manufacturer in Annex 6 initiated. These provisions draw a line between a 'single' sensor failure and 'other failures' (for example more than one sensor), which appears too simplistic to accommodate all possible valid functional safety designs for complex systems (which might, for example, employ redundant sensors/fail operational designs for certain aspects). **Recommend to leave the decision how to deal with sensor failures in a safe way to the functional safety strategy defined by the OEM for the specific system in order to not restrict system designs.**
Functional safety	Annex 6: Complex electronic (CEL) system audit as required for all CEL systems. The interpretation and application of this Annex might be inconsistent between different technical services. **Recommend to amend Annex 6 to ensure current best practice is applied consistently. See Section 4.4.1.**

System category: ACSF Category E	
Driver monitoring / system misuse	
Driver monitoring/ misuse prevention	5.6.1.2.6. requires a 'driver availability recognition system' that shall be able to detect that the driver is present and available to take over the steering. The text makes the implicit assumption that a driver's 'availability to take over the steering' can be derived from the fact that the driver is 'active'. Factors such as alertness and attentiveness are not considered. Also, it is not defined what level of activity is required for a system to conclude that a driver is 'active' (e.g. are infrequent head movements 'activity'). 5.6.1.2.6.2. requires a proposed driver inactivity span [3 minutes] after which a warning is issued. This time span appears to be derived from research that investigated the time for a driver to show signs of tiredness after the onset of a journey, rather than after the last sign of physical activity (ACSF-06-25). It is unclear, for example, how long after the last head movement a driver can be considered available to take over the steering. This requires further research. 5.6.1.3.1.7.: Information about the driver availability recognition system to be provided together with the documentation package required in Annex 6: Information. No guidance is given to how the technical service should assess this information. **Recommend to clearly define in the regulation what the responsibility of the driver is when using a Category E system: Monitoring the driving environment (SAE Level 2) or monitoring the system (SAE Level 3).** **Recommend to define a horizontal regulation on driver monitoring systems for different required levels of alertness. Also reference in UN Regulation 79 a level of driver monitoring that is appropriate to ensure that the driver performs the required actions (i.e. monitoring the driving environment or system). This will require further research to define appropriate criteria (activity, alertness, attentiveness, etc.), time spans and detection mechanisms.** **See Section 4.4.3 for more detail.**
Road type limitation	5.6.1.1.2. limits the system to dual carriageways with separation of traffic and no pedestrians/cyclist allowed. The apparent intention is to limit the system to motorway-type roads. It is unclear whether the definition achieves this aim considering the varying road layouts in different countries (dual-carriageways interrupted by roundabouts, for example). Not stated how this should be implemented, but assumed geo-fencing. **Recommend to consider adding to the definition that the road does not have crossings or roundabouts. Recommend to consider some verification of this requirement (test or documentation of strategy).**
Driver responsibilities	It is not clearly defined what the responsibility of the driver is for a Category E system: Monitoring the driving environment (SAE Level 2) or monitoring the system (SAE Level 3). **Recommend to clearly define in the regulation what the driver's responsibilities are**
Vehicle owner information	5.6. requires information regarding the transition procedure and consequences of delayed take-over of the steering in the owner's manual. **Recommend to also require clear guidance for the driver what their responsibilities are and what non-driving tasks are permissible/not permissible while using a Category E system.**
System status indication	5.6.1.1.7. requires optical signal for stand-by, active and failure. **No recommendation**

System category: ACSF Category E	
Tests	The draft currently does not require a test of the 'driver availability recognition system'. **Recommend to define and require an appropriate test (see comments above under Driver monitoring / system misuse – Driver monitoring/ misuse prevention).**
Transition demand and related safety manoeuvres	
Transition demand (TD)	5.6.1.4.: TD initiated if: Driver not present, driver unbuckled, driver not available, system boundaries will be reached shortly (e.g. maximum speed exceeded, lateral acceleration exceeded, lane marking missing), failures. Vehicle shall follow the desired path during TD. Minimum length required for TD is currently [4 seconds]; i.e. the driver needs to be ready to take back control after 4 seconds. 5.6.1.3.1.3. and 5.6.1.3.1.4.: Documentation of the TD strategy (system boundaries for TD) and the time foreseen for safe transitions to be submitted as part of Annex 6 documentation package. 5.6.1.4.6 and 5.6.1.4.7: Optical plus acoustic or haptic and deactivation of infotainment not relevant to driving. **Recommend to further investigate whether 4 seconds is sufficient time for a safe transition. This time value will be critical for system safety in many real-world scenarios and should be founded on scientific evidence that ensures a safe operation (see, for example,** (Merat *et al.*, 2014)**).**
Minimal risk manoeuvre (MRM)	5.6.1.5.: MRM initiated if driver does not react to TD. Manoeuvre defined by manufacturer, but must include activation of hazard warning lights. 5.6.1.3.1.5.: Documentation of the strategy to be submitted as part of Annex 6 documentation package. **No recommendations**
Emergency manoeuvre (EM)	5.6.1.6.: EM initiated if imminent danger of collision and time for safe transition too short. This manoeuvre can consist of protective braking and/or steering. 5.6.1.3.1.6.: Documentation of the strategy to be submitted as part of Annex 6 documentation package. 5.6.1.7.: Requires longitudinal speed control and emergency braking capabilities. These current requirements are rather unspecific (what are minimum performance criteria for detection and braking performance?) and do not fall within the scope of UN Regulation 79 (steering system). **Recommend to consider a different approach to regulating the longitudinal control. Potential solutions would be: more detailed performance criteria and worst case tests in this regulation, or a horizontal regulation on automated driving systems for higher category systems (B2, E).**

System category: ACSF Category E	
Tests	Annex 7 currently defines 10 tests, of which 7 tests are related to the transition demand and related safety manoeuvres: TR1, TR2, TR3, TR4, TR5, EM1, and EM2. TR1, TR2 and TR3 are related to lane keeping functionality, not lane changing. **Recommend to remove the requirement for these tests (but rather cover them under Category B2). See comments under Safety under normal operating conditions – Operating conditions / capabilities.** EM1 and EM2 are related to longitudinal control, which is not in scope of UN Regulation 79 (steering systems). See comments above under Transition demand and related safety manoeuvres – Emergency manoeuvre (EM). **If the tests are to be kept in this Regulation, recommend to define more prescriptive AEB tests to ensure reproducible assessment outcomes.**
Incidents	
Incident recording (DSSA)	5.6.1.8. requires a data storage system for ACSF (DSSA), which is intended to capture data to determine whether the ACSF has operated properly. 5.6.1.8.5. requires recording 'after a road accident'. No detailed triggering conditions (e.g. delta-v or peak acceleration levels) are defined. No other safety-relevant incidents other than collisions are covered. 5.6.1.8.5. defines the recording time as [30 seconds] prior and [10 seconds] after an incident. These time-spans might be too short to cover entirely the causation of complex cases (e.g. Did the driver monitoring system alert the driver repeatedly in the last minutes before the incident? When was the last driver activity recorded?) 5.6.1.8.2. defines the data to be recorded. The data fields as defined might not be sufficient to draw conclusions about causation of collisions or other safety critical incidents. **Recommend to expand the list of data items to be recorded in order to allow conclusions about a collision (direction of force, airbags deployed, time-acceleration profile, etc.) and relevant incident causation factors (driver monitoring data, system override by driver, information about automatic emergency manoeuvres, ACSF sensor discrepancies, relevant road scene interpretation data).** **Recommend to expand the recording time span before an incident to capture a comprehensive picture of the phase leading up to a collision (repeated driver monitoring system alerts before the incident, frequent sensor discrepancies due to failing sensor equipment, etc.).** **Recommend to define specific triggering criteria. Recommend to extend these criteria further than capturing only collisions: Capturing incidents such as near-miss events, emergency manoeuvres performed by the ACSF, or unexpected ACSF disengagements would allow an assessment of the real-world safety performance of an ACSF implementation before a large number of collisions occur if necessary (e.g. to decide on recall action).** **See Section 4.4.4 for more detail on incident recording.**

4.4 Summary of major issues identified

The following major issues were identified in the tables above:

1. Inconsistent interpretation and application of CEL Annex (Annex 6)
2. Safety under all real-world scenarios (operational safety)

3. Driver monitoring (The driver's role when using ACSF)
4. In-service safety performance

These issues are explained in more detail below. Recommendations of how to resolve them are described in Section 5.

4.4.1 Inconsistent interpretation and application of CEL Annex (Annex 6)

Section 3 shows clearly that to assure the safety of complex electronic (CEL) systems, an assessment of the development life cycle is required, which includes the processes and standards followed and verification of safety requirements (goals). Section 3 also identified that key aspects of an assessment should include:

- Hazard identification and risk assessment with focus on controllability and consideration of human factors in particular the Human Machine Interface (HMI)
- Management of safety requirements, in particular verification of them.

Annex 6 of UN Regulation 79 is effectively an audit, by the technical service, of the development life cycle or methodology used for the design of a 'complex electronic control system', to show the safety of the design (with verification) and in particular that 'the system' does not adversely affect the function of the main steering system in non-fault (i.e. normal) and fault operating conditions. It does not enforce any performance requirements, but plays a very important part in assuring the safety of ACSF which are complex electronic (CEL) systems.

For lower category systems (e.g. CSF, Cat B1), it was thought likely that current best practice implementation of Annex 6 together with the other requirements defined in the current draft should be sufficient to assure safe system function in all real-world driving situations. Indeed, it may also be sufficient to ensure that the project objective above is met for higher category systems (e.g. Cat B2, Cat E), although some additional requirements may be needed because the driver is not required to monitor the environment at all times.

However, interview with a number of technical services and manufacturers from the ACSF IWG indicated that there was inconsistent interpretation and application of Annex 6. Examples are:

- Section 3.4.4: '*the chosen analytical approach(es) shall be established and maintained by the manufacturer and shall be made open for inspection by the technical service at the time of type approval*'
  To meet the requirements of this section it is understood that some technical services conduct an audit to inspect items such as the safety approach at both the concept (vehicle) and system levels, whereas because this is not specifically required, other technical services do not.
- There are no requirements for reporting by the technical service and thus no requirements for traceability, e.g. versions of documents inspected during an audit at a manufacturer's site are coded and listed in the records of the technical service. As a result of this, it is understood that reporting is inconsistent between technical services.

To help resolve this issue, work was performed to establish 'best practice' for the assessment required by Annex 6 and proposals made for amendments to Annex 6 to help implement this 'best practice'. The results of this work and the proposed amendments are reported in Section 5.1.

It should be noted that Annex 6 from Regulation 79 is used in the following other Regulations:

- Verbatim, i.e. exactly the same wording:
  - Regulation 13 Annex 18; Heavy vehicle braking
  - Regulation 13H Annex 8; Braking of passenger cars
- Similar with small amount of text change:
  - Regulation (EU) 347/2012 Annex III; AEBS for trucks and buses
  - Regulation (EU) 406/2010 Annex VI; hydrogen powered vehicles

Therefore, ideally, any amendments made to Annex 6 in Regulation 79, should also be made to the equivalent Annexes in Regulations 13, 13H, 347/2012 and 406/2010.

4.4.2 Safety in all real-world scenarios (operational safety)

Annex 7 currently defines 10 tests. Whilst these tests can help to demonstrate the performance of the system to the technical service, because of their limited number, they cannot assure the safe operation of the system in the large variety of scenarios, configurations and environmental conditions encountered in the real-world. For lower category systems, which require hands-on the steering wheel and driver monitoring of the environment (e.g. CSF, B1), assurance of safe operation may be provided from the Annex 6 assessment (together with the other requirements defined in the current draft). However, for higher category systems which allow hands-off the steering wheel and monitoring of the system only, as opposed to monitoring of the environment, additional assurance to the Annex 6 assessment may be needed. This is because the driver may not be available to help deal with infrequent and emergency situations. Hence, the system has to deal with them autonomously at least for a limited time.

To address this issue a proposal for additional requirements for operational safety is discussed and made in Section 5.2.

4.4.3 Driver monitoring (The driver's role when using ACSF)

The role and responsibilities of the driver in automated driving systems are an ongoing topic of discussion within the research community and many issues surrounding this topic are not fully resolved. The emerging structure of the working document appears to draw a line between two types of systems: Those which continuously *assist* the driver (e.g. ACSF Category B1) and those which influence the movement of the vehicle for extended periods without further driver command (e.g. ACSF Category B2).

Category B1 systems (potentially combined with C or D) are defined as 'hands-on' systems, meaning the driver is required to permanently monitor the driving environment as if they were operating the vehicle manually, *and* be constantly available to intervene via steering wheel operation. This is necessary because a B1 system is not required to have any means to detect other vehicles or obstacles on the road. (If it is combined with ACC, it is still not able to detect all relevant objects.) The driver's role is equivalent to a SAE Level 2 system[8] (driver to monitor the driving environment and the driving automation system's performance).

To enforce this driver role for B1 systems, the working document requires a hands-on detection system that provides an optic and acoustic warning after the steering was not held for 15 or 30 seconds, respectively. Physical contact with the steering wheel is an important prerequisite to enable a driver to react promptly to the driving environment. Enforcement of steering wheel contact will also give conscientious drivers a strong indication of the expectation put on them to permanently remain in control of the vehicle.

However, in TRL's view, hands-on detection alone will not prevent all foreseeable misuse: Drivers can direct their gaze away from the road permanently and perform secondary tasks with one hand, which means activities such as reading/writing emails or other phone-related activities will not be prevented. Such behaviour is to be expected if drivers have the impression they can rely on the system to perform without intervention. This could present a safety risk in the real-world use of Category B1 systems and should be considered for safe system design.

Category B2 systems (potentially combined with C, D or E) are understood by TRL as 'hands-off' systems, meaning that the driver is *not* required to keep hold of the steering wheel while the system is active. These systems are required to monitor the front of the

[8] http://standards.sae.org/j3016_201609/

vehicle and react to preceding traffic and emergency situations. Nevertheless, the driver has a monitoring obligation with these systems, which is currently not clearly defined. The draft requires 'physical availability to respond to a transition demand from an ACSF system', which implies that the driver is only required as a fallback after a certain pre-warning phase. This role is equivalent to a SAE Level 3 system (driver to be fallback-ready for the dynamic driving task).

To enforce this driver role for B2 systems, the working document (ACSF-06-28, Paragraph 5.6.1.2.6.2.) makes the implicit assumption that a driver's 'availability to take over the steering' can be derived from the fact that the driver is 'active'. Two main issues are attached to this, which will need further research to be addressed:

- The term 'driver's activity' is not supported with clear requirements, i.e. what level of movement is required for a system to conclude that a driver is active (e.g. are infrequent head movements 'activity'?).
- Certain secondary activities might distract the driver too much to regain control in a short amount of time. To ensure a safe transition to the driver, more than mere 'physical availability' and 'activity' will be required: The driver has to be permanently alert and attentive to a certain degree in order to re-engage with the driving task. These factors are not monitored according to the current draft and it is not clear what activities are and are not permissible for the driver when using the system.

The proposed time span of driver inactivity after which a warning is issued is [3 minutes]. This appears to be derived from research that investigated the time for a driver to show signs of tiredness after the onset of a journey, rather than after the last sign of physical activity (ACSF-06-25). It is unknown, for example, how long after the last head movement a driver can be considered available to take over the steering. This might require further research.

The time span currently proposed for transition of control is [4 seconds] after an inactivity warning was issued to the driver. Research indicates that longer periods might be required for drivers to safely regain control: Timespans of 15 seconds might be necessary (see, for instance, (Merat *et al.*, 2014)). This value will be critical for system safety in many real-world scenarios and should be founded on scientific evidence that ensures a safe operation.

Resolving these issues related to the driver's role when using ACSF will require:

- input and further research from human factors experts; and
- development of technical requirements for driver monitoring systems that allow enforcement of the required behaviour for each ACSF category or SAE level.

Further considerations and a review of current driver monitoring technologies are provided in Section 5.3.2.

4.4.4 In-service safety performance

Automated driving systems are a novel technology and the requirements for higher level ACSF (Categories B2 and E) in UN Regulation 79 are currently being drafted without industry or regulators having access to existing implementations of these systems. This is an issue because performance requirements have to be developed without practical experience or knowledge of real-world safety risks. The complexity of the software algorithms and electronic systems involved adds to this issue and makes it virtually impossible for a regulator to foresee all potential safety issues. Therefore, the requirements and test procedures under UN Regulation 79 will ultimately always be subject to a certain level of uncertainty about their effectiveness in ensuring safe system operation in all real-world scenarios.

Note that no world region has yet found a suitable approach for regulating automated driving systems in a way that ensures upfront proof of safe system operation. If UN Regulation 79 attempts to define such an approach as a world first, it appears advisable to foresee a mechanism that allows swift monitoring of the actually achieved in-service safety performance of the approved vehicles. This would allow authorities to take

preventive steps before a large number of collisions occur in the field if, for instance, a faulty algorithm leads to erroneous lane change decisions of a Category E ACSF. The current mechanisms foreseen in the General Product Safety Directive and the vehicle recall procedures might not be fast enough for this purpose.

The mandatory incident recording mechanism (DSSA) could offer a potential route for a solution to this issue, but it would need certain modification with regard to the triggering criteria, the data recorded, and use of the data. TRL's proposed steps are discussed in Section 5.4.

5 Task 4: Identify additional test or certification requirements to ensure the system functionality is safe in all real world driving scenarios

5.1 Inconsistent interpretation and application of CEL Annex (Annex 6)

As mentioned previously in Section 4.4.1, Annex 6 is effectively an audit, by the technical service, of the development life cycle or methodology used for the design of a 'complex electronic control system', to show the safety of the design (with verification) and in particular that 'the system' does not adversely affect the function of the main steering system in non-fault (i.e. normal) and fault operating conditions. It does not enforce any performance requirements, but plays a very important part in assuring the safety of ACSF, which are complex electronic (CEL) control systems.

For lower category systems (e.g. CSF, Cat B1), it was thought likely that current best practice implementation of Annex 6 together with the other requirements defined in the current draft should be sufficient to assure safe system function in all real-world driving situations. This is because the driver is 'hands-on' and always 'in the loop' for these systems, assuming that he is not misusing the system, e.g. phone related activities with one hand – note that this is discussed further in Section 5.3 'Driver monitoring'. Therefore the driver should be in a position to take control of the vehicle when needed, e.g. in the case of infrequent and emergency events. For higher category systems (e.g. Cat B2, Cat E), some additional requirements are likely to be needed because the driver can be hands-off and may not be 'in the loop' and therefore may not be in a position to take immediate control of the vehicle. For the types of system currently under discussion within the ACSF group (SAE level 2), these requirements may include checks to ensure safety in the case of infrequent and/or emergency events (operational safety) and requirements for driver monitoring to ensure that the driver is at least monitoring the system performance.

5.15.1

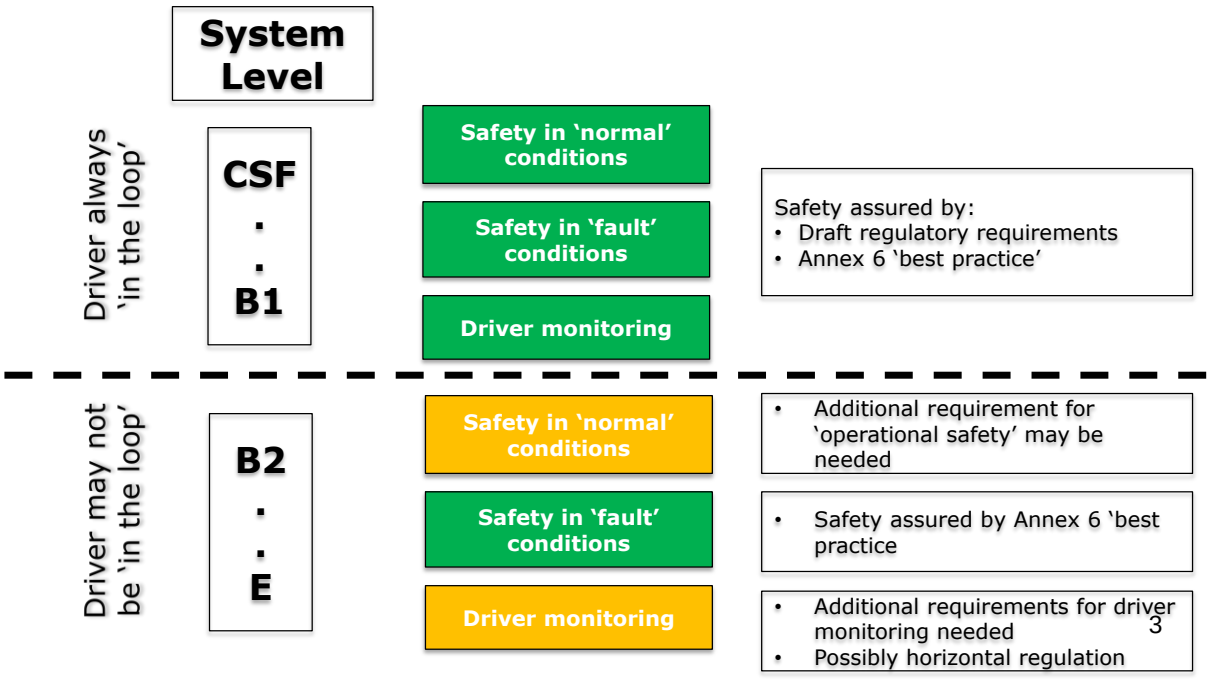

Figure 8: Rationale for application of 'best practice' Annex 6 to ACSF categories.

The current issue is that the Annex 6 assessment process is not consistent across technical services. This issue was raised by a number of technical services and manufacturers within the ACSF IWG.

The remainder of this section describes the work performed to establish 'best practice' for an Annex 6 assessment and proposed amendments developed to help implement this 'best practice'.

Best practice was established from interview of a number of technical services within Europe and active within the ACSF working group, namely those from France, Germany and the UK, and selected manufacturers. It was found that typical best practice implementation consisted of the following steps:

1. Initial meetings between TS and OEM (of the order of 6 months to 1-2 year before approval depending on complexity of system)

- Check if type-approval possible / applicable for the system; e.g. check conformity with Convention of Road Traffic, Vienna 1968
- Estimate complexity of the system and develop plan for approval of system

2. Functional safety analysis including audit (Annex 6, paragraph 3)

- Analysis of manufacturer supplied documentation to understand and check safety concept and prepare for audit
- Assessment of general development process; (an audit, usually at manufacturer's premises)
- Assessment of system development (an audit, usually at manufacturer's premises
    - Check safety approach at concept level (e.g. HAZOP)
    - Check safety approach at system level (e.g. FMEA and FTA)
    - Check validation plans
- As a result of audit, often recommendations are made for vehicle level tests to verify safety concept and check controllability

3. Functional safety assessment (Annex 6, paragraph 4)

- Verification of the function of the system
- Verification of the safety concept
- Provision for technical inspection

4. Compilation of technical report

Also noted were:

- The need for traceability to a level that the assessment could be repeated if necessary. This is particularly important for the assessment of confidential material usually carried out at the manufacturer's premises, documents checked should be coded and recorded.
- The importance of competent staff; without these a proper assessment is not possible. One technical service interviewed indicated that two areas of expertise were critical, namely electronic control systems and vehicle safety, and employed experts in both these areas to perform an assessment. However, this issues falls under Articles 41 (designation of technical services) and 42 (assessment of the skills of the technical services) of the framework Directive, see extracts below:
    - 41.4 Technical services shall demonstrate appropriate skills, specific technical knowledge and proven experience in the specific fields covered by this Directive and the regulatory acts listed in Annex IV.
    - 42.1 The skills referred to in Article 41 shall be demonstrated by an assessment report established by a competent authority. This may include a certificate of accreditation issued by an accreditation body.
- The German approval authority (KBA) requires that:
    - If a complex electronic control system cannot be covered entirely by a single Directive, but, due to its combined functionality, has to be judged applying 'general requirements' the technical service must be designated or accredited for the test of whole vehicles.
    - If more than one technical service is involved in a type-approval, test reports shall be exchanged directly between technical services (not via OEM) to avoid tampering.

- Within the Annex 6 assessment of the CEL system to environmental influence, in particular the type and scope of tests on climate and mechanical resistance and electromagnetic compatibility should be inspected.

From the above, the following changes to Annex 6 were identified as necessary to enforce best practice:

- Early involvement of TS in the development process to ensure good understanding of safety approach and concept
- 'Audit' of confidential documentation provided, usually performed on site at OEM or if necessary supplier. Audit should include:
  - Inspection of safety approach at both concept (e.g. HAZOP) and system level (e.g. FMEA, FTA). Check existence of documents/files, their history and (to a certain extent) the content of the documents/files.
    - Note: safety approach at concept level should include consideration of:
      - Risks driven by interaction of CEL system with other vehicle systems, e.g. effect of LKA on AEB and/or ACC and
      - Risks driven by reasonably foreseeable misuse by driver
- Traceability of work performed by technical service to level that would allow work to be repeated, e.g. versions of documents inspected are coded and listed
- Resistance to environmental influence, type and scope of tests on climate and mechanical resistance and electromagnetic compatibility should be inspected
- Possibly, include report template to assure all aspects addressed; an example of a template produced by the German approval authority KBA is available publicly for information
- include report template to assure all aspects addressed;

Another important point for amendments to the regulation, perhaps outside the scope of Regulation 79 alone, is:

- **Staff competence**: This is critical to enable a 'best practice' assessment but currently enforced by Articles 41 and 42 of Framework Directive for EU and under discussion in the 1958 Agreement revision 3 draft

Proposals for amendments to the Annex 6 regulatory text were developed to implement the changes listed above and help implement current best practice. These are shown in Annex 1. These proposals were presented at the 82nd session of GRRF in Geneva by an expert from the European Commission (see documents GRRF-82-18 and GRRF-82-19).

5.2 Safety in all real-world scenarios (operational safety)

In this section, potential additional requirements to assure safety in all real-world scenarios are discussed and recommendations for modifications to Regulation 79 are proposed.

This section is divided into the following four sub-sections:

- Background
  - In this sub-section two recently published documents are reviewed briefly, namely:
    - Federal Automated Vehicles Policy
    - WP.29 ITS/AD IWG document: A proposal for the definitions of automated driving under WP.29 and the general principles for developing a UN Regulation
- Approach
  - The issue of if a B2 category system is an SAE level 2 or 3 system and its implications for operational safety are discussed. An approach for the way forward is proposed.
- Proposal for additional requirements for operational safety
  - An initial proposal for requirements to assure safety in all real-world scenarios is made for Cat B2 (and E) 'level 3' systems.

- Summary and recommendations for way forward

5.2.1 Background

5.2.1.1 Federal Automated Vehicles Policy

In September 2016, NHTSA issued a policy to help speed the delivery of an initial regulatory framework and best practices to guide manufacturers in the safe design, development, testing and deployment of Highly Automated Vehicles (HAV) (NHTSA, 2016). This policy consists of four sections:

- Vehicle Performance Guidance for Automated Vehicles
- Model State Policy
- NHTSA's Current Regulatory Tools
- New Tools and Authorities

Vehicle Performance Guidance for Automated Vehicles:

The vehicle performance guidance section highlights areas that manufacturers and other entities should consider and address as they design, test and deploy HAVs. For all HAV systems the manufacturer should address the cross-cutting items as a vehicle or equipment is designed and developed to ensure that the vehicle has data recording and sharing capabilities; that it has applied appropriate functional safety and cybersecurity best practices; that HMI design best practices have been followed; that appropriate crashworthiness/occupant protection has been designed into the vehicle; and that consumer education and training have been addressed (see Figure 9).

In addition to the cross-cutting areas, for each specific HAV system, the manufacturer should define the operational design domain (ODD). Definition of the ODD is necessary to determine what object and event detection (OEDR) capabilities are required for the HAV to operate safely within the ODD. OEDR requirements are derived from an evaluation of normal driving scenarios, expected hazards (e.g., other vehicles, pedestrians), and unspecified events (e.g., emergency vehicles, temporary construction zones) that could occur within the operational domain.

The fall back minimal risk condition portion of the framework is also specific to each HAV system. Defining, testing, and validating a fall back minimal risk condition ensures that the vehicle can be put in a minimal risk condition in cases of HAV system failure or a failure in a human driver's response when transitioning from automated to manual control.

Finally, tests should be developed and conducted that can evaluate (through a combination of simulation, test track or roadways) and validate that the HAV system can operate safely with respect to the defined ODD and has the capability to fall back to a minimal risk condition when needed.

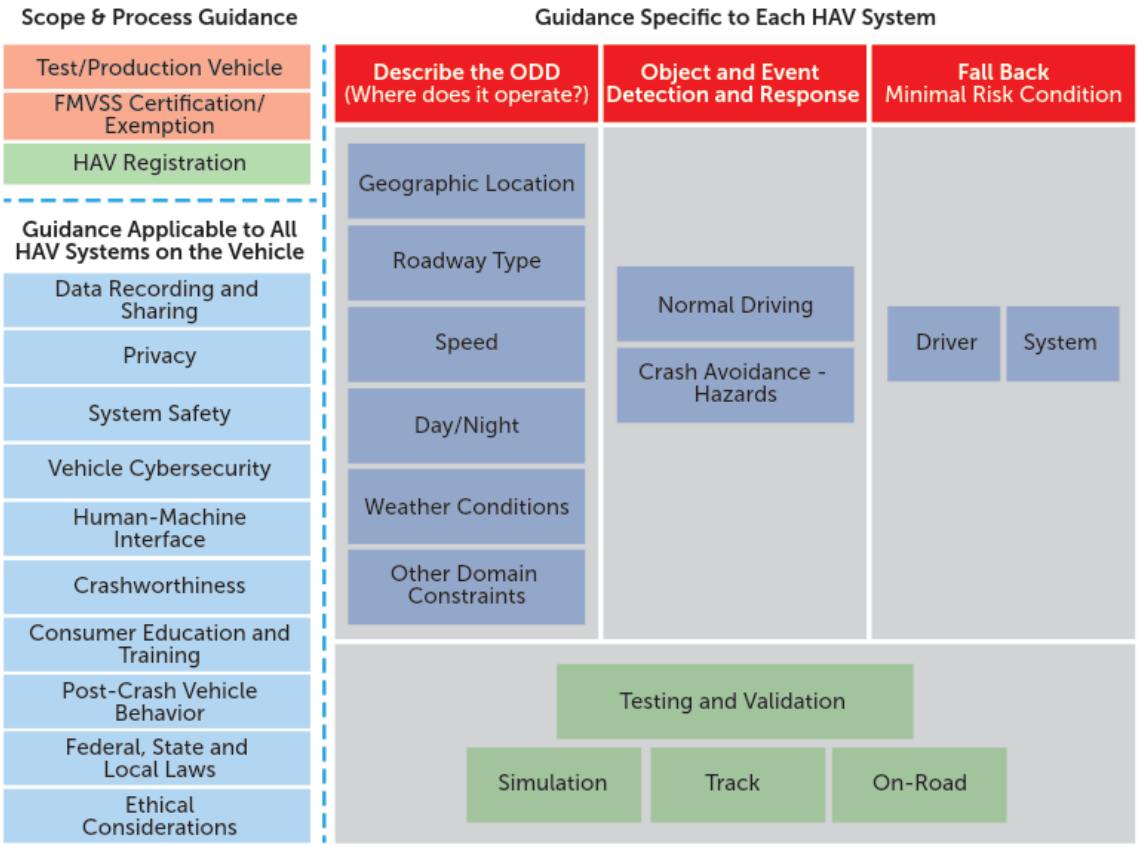

Figure 9: Federal automated vehicles policy: Framework for vehicle performance guidance.

To aid NHTSA in monitoring HAVs, the guidance states that the Agency will request that manufacturers and other entities voluntarily provide reports regarding how the guidance has been followed. In the future, it is anticipated that this reporting process may be refined and made mandatory through future rulemaking. It is expected that this would require submission of a safety assessment to NHTSA by the manufacturer which outlines how the guidance is met for each HAV system. The assessment should include a signed acknowledgment (declaration) by an authorised company official for each guidance area as follows:

- Meets guidance area
- Does not meet guidance area
- Guidance area not applicable

Model State policy

The objective of this part of the federal policy is to ensure the establishment of a consistent national framework rather than a patchwork of incompatible laws. State governments play an important role in facilitating HAVs, ensuring they are safely deployed, and promoting their life-saving benefits. The Model State Policy confirms that States retain their traditional responsibilities for vehicle licensing and registration, traffic laws and enforcement, and motor vehicle insurance and liability regimes.

NHTSA's current regulatory tools:

NHTSA's current regulatory tools do not prohibit the introduction of new motor vehicles or motor vehicle technologies into the vehicle fleet, provided that those vehicles and technologies meet existing Federal Motor Vehicle Safety Standards (FMVSS). A vehicle or equipment manufacturer need ask NHTSA about a new technology or vehicle design only when it will not comply with applicable standards, or when there might be a question as to compliance. If a manufacturer anticipates having such a question, then requests for

interpretations, exemptions, and rulemakings are the methods that a manufacturer can use to pursue answers from the Agency. Current tools include:

- Letters of interpretation
    - Interpretation of Agency's view of how existing law applies to requestor's motor vehicle or motor vehicle equipment
    - Response to a HAV related interpretation request that appears to improve safety – NHTSA will endeavour to give quicker responses; simple request 60 days, more complex 90 days.
- Exemptions from current standards
    - Intended to provide some flexibility to general requirement that manufacturers must comply with applicable FMVSS and bumper standards
    - General exemptions are temporary (1 to 2 years) and may be granted for the following reasons:
        - Substantial economic hardship
        - Development or field evaluation of a new motor vehicle safety feature (for up to 2,500 vehicles per year)
        - Development or field evaluation of a low-emission motor vehicle (for up to 2,500 vehicles per year)
        - Overall safety level of exempted vehicle at least equal to overall safety level of non-exempt vehicles (for up to 2,500 vehicles per year).
- Rulemaking to amend existing standards or create new standards
- Enforcement authority to address defects that pose unreasonable risk to safety
    - This includes those related to new and emerging technologies such as HAVs.

New tools and authorities

This section discussed potential new tools and authorities that could help to meet the challenges and opportunities involved in facilitating the safe, expeditious development of HAVs. Points discussed included:

- The importance of research to guide regulatory actions
- Potential new authorities
    - Safety assurance rules which could require manufacturers to provide advance information about their efforts to ensure safe introduction of HAVs, e.g. as in vehicle performance guidance section above.
    - Pre-market approval authority approach which could involve an approach similar to that of the Federal Aviation Authority, which requires a 'type certification' five phase process for approving aircraft design from early project concept and initiation through to post certification activities.
    - Cease-and-Desist authority which could enable NHTSA to require manufacturers to take immediate action to mitigate safety risks that are so serious and immediate as to be imminent hazards.
    - Expanded exemption authority for HAVs, which could expand the Agency's authority which currently stands at 2,500 vehicles per year for a two-year period, on the basis of equivalent safety.
    - Post-sale authority to regulate software changes which may need the development of additional regulatory tools.
- Potential new tools
    - Variable test procedures to ensure behavioural competence and avoid gaming of tests
    - Functional and system safety
    - Regular reviews for making agency testing protocols
    - Additional record keeping / reporting
    - Enhanced data collection tools
- Agency resources
    - Network of experts
    - Special hiring authority

5.2.1.2 WP.29 ITS/AD IWG discussion / proposal document

The WP.29 ITS/AD informal working group has developed, 'A proposal for the definitions of automated driving under WP.29 and the general principles for developing a UN Regulation'[9]. The proposal consists of a table which classifies levels of automated driving using the SAE definitions and considers various points against these classifications such as driver actions (permitted and not permitted) and system requirements (unnecessary or what's required). For example, for SAE levels 1 and 2, monitoring of the environment by the driver is required and the driver may not perform secondary tasks. For SAE levels 3, 4 and 5 the environment is monitored by the system and the driver may perform a secondary task. However, to allow this safely, examples of necessary system performance requirements are defined such as comprehensive recognition of the surrounding environment in lateral and longitudinal directions.

It is interesting to note that in the section which summarises the current conditions and issues to be discussed, ACSF Cat. B2 and E, which allow hands-off driving while the system is active, are classified as level 2(b) systems in which the driver must monitor the environment and is not allowed to perform secondary tasks.

In the current draft working document Cat B2 and E systems are required to monitor the front of the vehicle and react to preceding traffic and emergency situations. Nevertheless, the driver has a monitoring obligation with these systems, which is currently not clearly defined. The draft requires: 'physical availability to respond to a transition demand from an ACSF system', which implies that the driver is only required as a fallback after a certain pre-warning phase. This role is equivalent to a SAE Level 3 system (driver to monitor the system). This does not fit with the current classification of these systems (B2 and E) as level 2(b).

Another point to note is that the Federal Automated Vehicles Policy discussed above puts specific emphasis on driver complacency and foreseeable misuse of level 2 systems and states:

Manufacturers and other entities should place significant emphasis on assessing the risk of driver complacency and misuse of Level 2 systems, and develop effective countermeasures to assist drivers in properly using the system as the manufacturer expects. Complacency has been defined as, "… [when an operator] over-relies on and excessively trusts the automation, and subsequently fails to exercise his or her vigilance and/or supervisory duties"

5.2.2 Approach

As mentioned above in Section 5.1, for lower category systems (e.g. CSF, Cat B1), it was thought likely that current best practice implementation of Annex 6 together with the other requirements defined in the current draft should be sufficient to assure safe system function in all real-world driving situations. This is because the driver is 'hands-on' and always 'in the loop' for these systems, assuming that he is not misusing the system, e.g. phone related activities with one hand. Best practice implementation of Annex 6 includes assessment of the safety concept to prevent foreseeable misuse. Therefore the driver should be in a position to take control of the vehicle when needed, e.g. in the case of infrequent and emergency events. For higher category systems (e.g. Cat B2, Cat E), some additional requirements are likely to be needed because the driver can be hands-

[9] Document No. ITS/AD-AH-01-03-Rev3.

https://www2.unece.org/wiki/download/attachments/36897054/%28ITS_AD-AH-01-03-Rev3%29%20The%20Definitions%20of%20Automated%20Driving%20under%20WP.29%20and%20the%20General%20Principles%20for%20developing%20a%20UN%20Regulation-Rev3.pdf?api=v2

off and may not be 'in the loop' and therefore may not be in a position to take immediate control of the vehicle.

For cat B2 and E systems, it is TRL's understanding that 'hands-off' operation is permitted. The current proposal (ACSF-06-28) requires permanent driver monitoring to detect driver's activity and if no activity is detected for a time span of maximum 3 minutes, a warning will be provided until appropriate actions of driver are detected or if not, after 15 seconds a transition demand is initiated. These requirements could allow the driver to be 'out of the loop' for 3 minutes or slightly more. During this time the driver may not be monitoring the environment. This could be because of complacency and /or misuse (e.g. performing secondary tasks even though TRL understand that this is not permitted because it is a level 2 system). In contrast for B1 systems, which only allow hands-on operation, a warning is given after 15 seconds if it is detected that the driver is not holding the steering wheel. Because the driver may not be available to take over control for a period of up to 3 minutes or more TRL recommend that requirements similar to those for a level 3 system should be imposed. Document ITS/AD-AH-01-03-Rev3 gives a description of requirements for a level 3 system as follows:

the system shall be able to cope with any situations within the concerned use case which includes the period of transition to driver control, the system drives and monitors the environment and is able to warn the driver sufficiently in advance if a takeover is necessary in the use case.

To ensure these requirements are met would need a comprehensive assessment of safety within the concerned use case for normal driving for category B2 systems. What this may constituent is described further in Section 5.2.3 below.

Alternatively, if only 'hands-on' operation for Cat B2 systems was to be permitted as for Cat B1 systems and a warning is given after 15 seconds if it is detected that the driver is not holding the steering wheel, the driver may be 'out of the loop' for 15 seconds only. In this case the system need not be able to cope with all situations within the concerned use case because the driver should be available. In this case assessment of safety within the concerned use case for normal driving may not be needed. However, because the Cat B2 system may reduce workload more than a Cat B1 system, some additional requirements may be prudent, such as an enhanced driver monitoring system (i.e. additional monitoring to hands-on detection) and a minimum risk manoeuvre requirement, to offset the additional risk of driver complacency and misuse.

It should be noted that the modifications to Annex 6 proposed above already include consideration of driver complacency and foreseeable misuse, as part of safety approach assessment, in particular the safety approach at the concept (vehicle) level and HAZOP analysis.

It is interesting to note that it is reported that Tesla will upgrade their Autopilot system such that the new v8.0 software will give more weight to 'hands-off' alerts by adding a restriction that will result in not only the Autopilot disengaging after alerts are repeatedly ignored, but also blocking the driver from re-engaging the feature after it is automatically disengaged until the vehicle stops and is put in 'park'[10]. This illustrates the need to consider additional counter-measures for driver complacency and misuse of the system.

5.2.3 Proposal for additional requirements for operational safety for Cat B2 (and E) systems

Operational safety is defined as safety in normal (non-fault) operating conditions, including the HMI, in the concerned use case (also referred to as the Operational Design Domain (ODD)) – see illustration in Figure 10.

[10] Online Electrek article (August 28th 2016): https://electrek.co/2016/08/28/tesla-autopilot-safety-restrictions-v8-0-accidents/

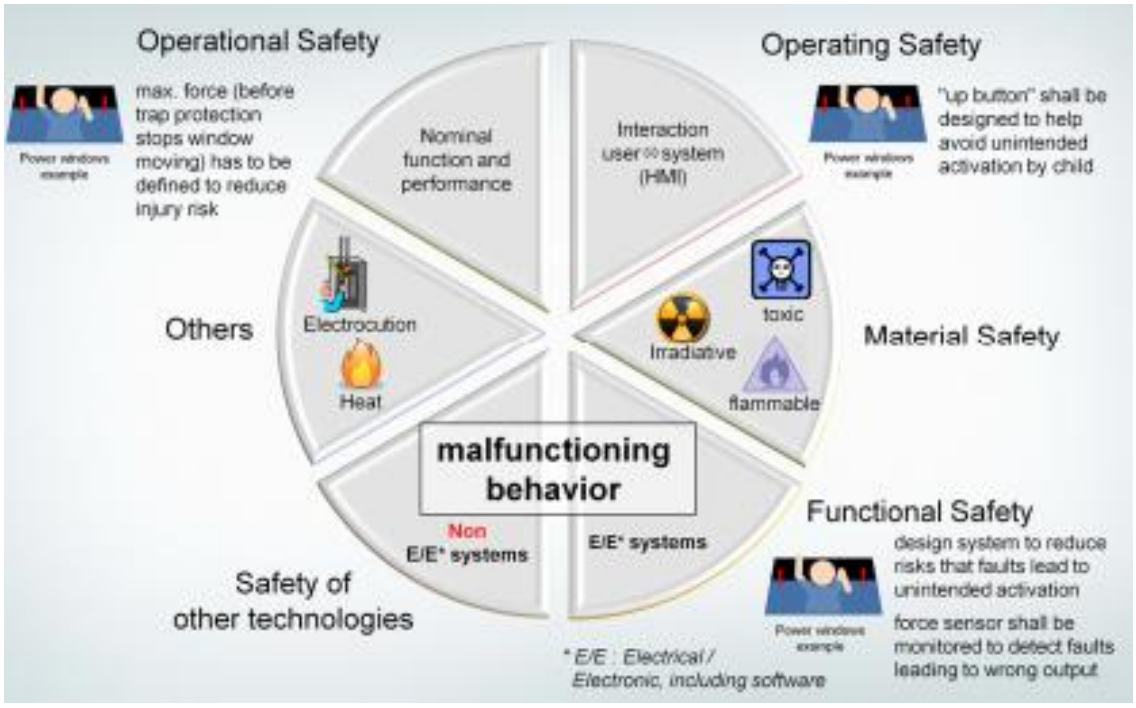

Figure 10: Definition of 'operational safety', top two sections of pie, 'nominal function and performance and interaction (HMI)' in ODD. Source: ACSF IWG industry representatives.

An initial list of areas to be considered for assessment of safety in normal (non-fault) operating conditions has been generated and is shown in the bullet pointed list below. It was generated using information from discussions within the ACSF IWG and a comparison of requirements in the Federal Automated Vehicles Policy and the Regulation 79 draft amendments (see Table 12 below). Comments *in italics* are included where areas may be partially covered by the current Annex 6, the Annex 6 amendments proposed above (Section 5.1), and/or other currently proposed Regulation 79 amendments.

- Submission of documentation describing the development process for the assessment, testing and validation of 'operational safety', i.e. safety in full range of real-world normal operating conditions, including HMI.
- Submission of documentation which describes the approach used and verification performed to assure safe operation in the full range of real-world conditions which may occur in the concerned use case (operational design domain (ODD)) including but not limited to:
    - General
        - Different environmental conditions, road, weather, etc.
            - Roadway types, geographic area, speed range, environmental conditions (weather, daytime / nighttime, etc.)

            (Note: this may be covered partially as part of Annex 6 assessment, e.g. speed range of ODD, geo-fencing, etc.).

        - Driver complacency and misuse.
            - Effective countermeasures to ensure drivers use the system properly as expected and designed by the manufacturer.

            (Note: this may be covered as part of Annex 6 proposed amendments as part of vehicle concept level HAZOP analysis)

    - Object and event detection and response including but not limited to:
        - Detect and respond to stopped or rapidly slowing vehicle in front

(Note: Annex 7 tests cover this partially – tests EM1 & EM2. To ensure covered fully, one option is that the Annex 7 could be amended to add requirement for: 'Documentation demonstrating compliance for range of vehicles and slowing'.)

- Detect and respond to other vehicles changing lanes
- Detect and respond to roadworks
- Detect and respond to emergency vehicles
- Detect and respond to animals / pedestrians in the road
- Detect and respond to static objects (e.g. debris) in the road

  - Minimal Risk Manoeuvre (MRM)
    (*Note: MRM already included in main text of Regulation*)

- Declaration signed by an authorised company official and dated stating that documented development process followed to assess and verify that the system should operate safely within its ODD in normal (non-fault) operating conditions and that the state of the art engineering practices have been applied.

The requirements listed above could be included in Regulation 79 in the following manner:

1. As an Annex for 'operational safety' (safety in normal (non-fault) operating conditions, including HMI).
2. As individual requirements within the main text of Regulation 79.
3. As a combination of 1 and 2.

Table 12: Comparison of requirements in Federal Automated Vehicles Policy and Regulation 79 draft amendments for ACSF.

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement *Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	Equivalency and comment / recommendation
Safety assessment area	Requirement outline		
1. Data recording and sharing	Collection of event, incident and crash data	5.6.4.8 (DSSA): Collection of crash event data	Not equivalent. Recommend to include collection of event and incident data in R79.
2. Privacy	Steps to protect consumer privacy	5.6.4.8.1 (DSSA) Designed to ensure data security and data protection	Requirements generally equivalent.
3. System safety	Robust design and validation approach which includes fail safe requirement.	Annex 6 requirements for CEL systems (with amendments recommended in this report).	Requirements generally equivalent.
4. Vehicle cyber-security	Robust product development process including ongoing systematic risk assessment to minimise cybersecurity risks to safety. Evolving area in which further research is necessary so manufacturers should incorporate current best practices / guidelines.	Not covered	Area not covered in R79 and largely outside scope of current R79 amendments. Will most likely be included in horizontal regulation.
5. Human machine interface	Documented process for the assessment, testing and validation of the vehicle HMI.	Annex 6 requirements for CEL systems (with amendments recommended in this report)	Requirements generally equivalent.
6. Crashworthiness	Meet current federal crashworthiness standards	Meet current EU crashworthiness standards	Requirements generally equivalent.
7. Consumer education and training	Manufacturers should develop and maintain consumer education and training programs to give users the necessary level of understanding to use these technologies properly.	Not covered	Consideration of consumer education may be needed for higher level HAV systems (4 & 5). However, these are largely outside the scope of current amendments.
8. Registration and certification	Communication of information to indicate HAV capability and any changes to it throughout vehicle life	Not covered	Issue outside the scope of current R79 amendments.
9. Post-crash behaviour	If sensors or critical safety control systems are damaged vehicle not permitted to operate vehicle in HAV mode.	5.6.4.1 (General) System shall only operate if all associated functions are working properly. Annex 6 requirements for CEL systems(with amendments recommended in this report).	Requirements generally equivalent.

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement *Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	Equivalency and comment / recommendation
Safety assessment area	Requirement outline		
10. Federal, state and local laws	Based on the ODD, the HAV should obey local traffic laws and follow the rules of the road for the region of operation.	5.6.4.1.4 Maximum speed of operation of system of 130 km/h, which helps meet traffic laws. 5.6.1.1.x (Cat E only, no requirement for Cat B2) Vehicle shall detect max speed limit of country and not activate system above this value.	Requirements generally equivalent.
11. Ethical considerations	Decisions made by HAV driver will have ethical dimensions which should be made consciously and intentionally.	Not covered	Issue outside the scope of current R79 amendments.
12. Operational Design Domain (ODD)	**ODD** The defined ODD should include the following: • Roadway types on which HAV system is intended to operate safety • Geographic area • Speed range • Environmental conditions • Other domain constraints **Safe operation within ODD** For each HAV system the manufacturer should have a documented process for the assessment, testing and validation of the system's capabilities. Manufacturer should apply tests and standards to establish safe operation of HAV system within ODD. **Transition** Outside ODD or in cases in which conditions dynamically change to fall outside ODD, vehicle should transition to a minimal risk condition and give clear indication that system is not available.	**ODD** 5.6.4.2.1 System shall only operate if: • Travelling on road section which is not dedicated to pedestrians or bicyclists and has physical separation of traffic moving in opposite directions 5.6.4.3 System information data to be supplied as part of Annex 6 documentation package. • Values for min/max speed and max lateral acceleration. **Safe operation within ODD** • Annex 7 tests, but no other requirements **Transition** 5.6.4.4 Transition demand and system operation during transition Various details for transition demand for driver to take control and vehicle actions during this period. 5.6.4.5 to 7 Minimal risk and emergency	**ODD** Recommend consideration of refinement of definition for ODD **Safe operation within ODD** Recommend consideration of additional requirements for documented process and check of tests applied by manufacturer to establish safe operation of system within ODD. **Transition** Requirements generally equivalent.

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement *Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	Equivalency and comment / recommendation
Safety assessment area	Requirement outline		
		manoeuvres and protective deceleration. Requirement for minimal risk and emergency manoeuvres for situations when driver not able to take control. Also requirement for longitudinal control which is necessary to enable min risk and emergency manoeuvres. Annex 7 minimum and emergency manoeuvre tests.	
13. Object and event detection and response	Entities should have a documented process for assessment, testing and validation of their OEDR capabilities. OEDR functions should be able to detect and respond to other vehicles (in and out of its travel path), pedestrians, animals, other objects, etc. that could affect safe operation. Within ODD, HAV should be able to deal with variety of conditions including emergency vehicles, temporary work zones and other unusual conditions that may impact safe operation.	No requirement for documented process. 5.6.4.2.1 System shall only operate if: Any traffic that can affect safety is identified and its speed / distance can be analysed to ensure safety (e.g. does not have adverse effect on other traffic). 5.6.4.5 to 7 Minimal risk and emergency manoeuvres and protective deceleration. Requirement for minimal risk and emergency manoeuvres for situations when driver not able to take control. Also requirement for longitudinal control which is necessary to enable min risk and emergency manoeuvres. Annex 7 minimum and emergency manoeuvre tests.	Recommend consideration of additional requirements for documented process and check of tests applied by manufacturer to validate OEDR capabilities.
14. Fall back (minimal risk condition)	Documented process for transitioning to minimal risk condition or proper control by driver when a problem is encountered, e.g. malfunction, operating outside ODD.	5.6.4.5 Minimal risk manoeuvre 5.6.4.4 Transition demand and system operation during transition	Requirements generally equivalent.
15. Validation methods	Tests and validation methods to ensure a high level of safety in the operation of their HAVs, for normal operation, during crash avoidance	Annex 7 tests.	Recommend consideration of additional requirements for documented process and check of

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement *Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	Equivalency and comment / recommendation
Safety assessment area	Requirement outline		
	situations and fall back strategies relevant to ODD.		tests applied by manufacturer to establish safe operation of system within ODD.
Safety assessment area	Requirement outline	Working draft Regulation 79 draft amendments for ACSF equivalent requirement *Paragraph references given for Cat B2.	Comment / recommendation
1. Data recording and sharing	Collection of event, incident and crash data	5.6.4.8 (DSSA): Collection of crash event data	Recommend to include collection of event and incident data
2. Privacy	Steps to protect consumer privacy	5.6.4.8.1 (DSSA) Designed to ensure data security and data protection	Issue seems to be correctly covered for level 3 systems. No recommendation.
3. System safety	Robust design and validation approach which includes fail safe requirement.	Annex 6 requirements for CEL systems	Area generally covered for level 3 system, no recommendation.
4. Vehicle cyber-security	Robust product development process including ongoing systematic risk assessment to minimise cybersecurity risks to safety. Evolving area in which further research is necessary so manufacturers should incorporate current best practices / guidelines.	Not covered	Too early to propose requirement, no recommendation.
5. Human machine interface	Documented process for the assessment, testing and validation of the vehicle HMI.	Annex 6 requirements for CEL systems	Area generally covered for level 3 system, no recommendation.
6. Crashworthiness	Meet current federal crashworthiness standards	Meet current EU crashworthiness standards	Requirements similar, no recommendation
7. Consumer education and training	Manufacturers should develop and maintain consumer education and training programs to give users the necessary level of understanding to use these technologies properly.	Not covered	Consideration of consumer education may be needed for higher level HAV systems (4 & 5). However, these are largely outside the scope of current amendments.
8. Registration and	Communication of information to indicate HAV capability and any changes to it throughout	Not covered	Issue outside the scope of current

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement *Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	Equivalency and comment / recommendation
Safety assessment area	Requirement outline		
certification	vehicle life		amendments.
9. Post-crash behaviour	If sensors or critical safety control systems are damaged vehicle not permitted to operate vehicle in HAV mode.	5.6.4.1 (General) System shall only operate if all associated functions are working properly. Annex 6 requirements for CEL systems.	Requirements similar, no recommendation
10. Federal, state and local laws	Based on the ODD, the HAV should obey local traffic laws and follow the rules of the road for the region of operation.	5.6.4.1.4 Maximum speed of operation of system of 130 km/h, which helps meet traffic laws. 5.6.1.1.x (Cat E only, no requirement for Cat B2) Vehicle shall detect max speed limit of country and not activate system above this value.	Area generally covered for level 3 system, no recommendation.
11. Ethical considerations	Decisions made by HAV driver will have ethical dimensions which should be made consciously and intentionally.	Not covered	Issue outside the scope of current amendments.
12. Operational Design Domain (ODD)	The defined ODD should include the following: • Roadway types on which HAV system is intended to operate safety • Geographic area • Speed range • Environmental conditions • Other domain constraints For each HAV system the manufacturer should have a documented process for the assessment, testing and validation of the system's capabilities. Manufacturer should apply tests and standards to establish safe operation of HAV system within ODD. Outside ODD or in cases in which conditions dynamically change to fall outside ODD, vehicle should transition to a minimal risk condition and	ODD 5.6.4.2.1 System shall only operate if: • Travelling on road section which is not dedicated to pedestrians or bicyclists and has physical separation of traffic moving in opposite directions 5.6.4.3 System information data to be supplied as part of Annex 6 documentation package. • Values for min/max speed and max lateral acceleration. Safe operation within ODD • Annex 7 tests, but no other requirements Transition 5.6.4.4 Transition demand and system operation	ODD Recommend consideration of additional definitions for ODD Safe operation within ODD Recommend consideration of additional requirements for documented process and check of tests applied by manufacturer to establish safe operation of system within ODD. Transition Area generally covered for level 3 system. No recommendation.

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement	Equivalency and comment / recommendation
Safety assessment area	Requirement outline	*Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	
	give clear indication that system is not available.	during transition Various details for transition demand for driver to take control and vehicle actions during this period. 5.6.4.5 to 7 Minimal risk and emergency manoeuvres and protective deceleration. Requirement for minimal risk and emergency manoeuvres for situations when driver not able to take control. Also requirement for longitudinal control which is necessary to enable min risk and emergency manoeuvres. Annex 7 minimum and emergency manoeuvre tests.	
13. Object and event detection and response	Entities should have a documented process for assessment, testing and validation of their OEDR capabilities. OEDR functions should be able to detect and respond to other vehicles (in and out of its travel path), pedestrians, animals, other objects, etc. that could affect safe operation. Within ODD, HAV should be able to deal with variety of conditions including emergency vehicles, temporary work zones and other unusual conditions that may impact safe operation.	No requirement for documented process. 5.6.4.2.1 System shall only operate if: Any traffic that can affect safety is identified and its speed / distance can be analysed to ensure safety (e.g. does not have adverse effect on other traffic). 5.6.4.5 to 7 Minimal risk and emergency manoeuvres and protective deceleration. Requirement for minimal risk and emergency manoeuvres for situations when driver not able to take control. Also requirement for longitudinal control which is necessary to enable min risk and emergency manoeuvres. Annex 7 minimum and emergency manoeuvre tests.	Recommend consideration of additional requirements for documented process and check of tests applied by manufacturer to validate OEDR capabilities.
14. Fall back (minimal risk	Documented process for transitioning to minimal risk condition or proper control by driver when a	5.6.4.5 Minimal risk manoeuvre	Requirements similar, no

Federal Automated Vehicles Policy		Regulation 79 draft amendment equivalent requirement *Note: Paragraph references given for Cat B2, a similar reference structure is used for Cat E.	Equivalency and comment / recommendation
Safety assessment area	Requirement outline		
condition)	problem is encountered, e.g. malfunction, operating outside ODD.	5.6.4.4 Transition demand and system operation during transition	recommendation
15. Validation methods	Tests and validation methods to ensure a high level of safety in the operation of their HAVs, for normal operation, during crash avoidance situations and fall back strategies relevant to ODD.	Annex 7 tests.	Recommend consideration of additional requirements for documented process and check of tests applied by manufacturer to establish safe operation of system within ODD.

5.2.3.1 'Traffic Jam Assist'

In the light of the potential list of requirements for operational safety above, it is interesting to consider 'Traffic Jam Assist' systems. If their operational design domain (ODD) is restricted to 'highways' only, these systems will fall into the B2 'level 3' category even though they may only operate up to speeds of about 25 - 30 km/h. Cat B2 systems explicitly include a 'highway' ODD within the definition (specifically Section 5.6.4.2.1 '*The ACSF system of category B2 shall only operate if the vehicle is travelling on a road section which is not dedicated to pedestrians or bicyclists and which has a [physical or constructional] separation of traffic moving in opposite directions'*. For systems like this the operational safety requirements listed above may appear too stringent and onerous. One could envisage that a system with lane following and AEB (with pedestrian capability) alone may be sufficient to assure safety.

However, it is possible that the ODD of these systems could include major roads other than highways in which there may be no physical separation of traffic moving in opposite directions, bicyclists are permitted and/or traffic lights may be present, etc. In this case, 'Traffic Jam Assist' systems would not fall under the B2 category and a separate ACSF category would need to be formed to regulate them, which would need to include a modified list of requirements for operational safety.

In light of these issues, it is recommended that the potential list of requirements in the section above be considered for all Cat B2 (and E) systems. If it is judged too stringent for traffic jam assist systems or traffic jam assist systems do not fulfil the Cat B2 'highway' ODD requirements, it is recommended that a specific ACSF category should be formed to regulate them.

5.2.4 Summary and recommendations for way forward

For Cat B2 systems, it is TRL's understanding that in the current ACSF IWG proposal (ACSF-06-28) 'hands-off' operation is permitted. The current proposal also allows up to about three minutes in which the driver may be 'out of the loop' and may not be monitoring the environment. Therefore, for this period the system must be capable of controlling the vehicle. On this basis TRL recommend that requirements similar to those for a level 3 system should be imposed, in particular:

- System shall be able to cope with any situations within the concerned use case which includes the period of transition to driver control, the system drives and monitors the environment and is able to warn the driver sufficiently in advance if a takeover is necessary in the sue case. The system detects system limits and issues a transition demand if these are reached. (Doc ITS/AD-AH-01-03)
- And thus a comprehensive assessment of safety within concerned use case for normal (non-fault) driving is required, i.e. operational safety.

Alternatively, if only 'hands-on' operation for Cat B2 systems is permitted and measures are taken to ensure that the driver is always 'in the loop' and monitoring the environment, as for a Cat B1 system, assessment of safety within the relevant use case for normal driving may not be needed. However, because the Cat B2 system may reduce workload more than a Cat B1 system, some additional requirements may be prudent, such as an enhanced driver monitoring system and a minimum risk manoeuvre requirement, to offset the additional risk of driver complacency and misuse.

Because a Cat B2 'hands-on' system would offer little advantage to the driver compared to a Cat B1 system, and indeed it may be approved as a B1 system, TRL believe that the only viable way forward is to consider a Cat B2 system as a level 3 'hands-off' system and add requirements for a comprehensive assessment of safety within relevant use case for normal (non-fault) driving, i.e. operational safety. This could be achieved either by:

- Additional requirements in Regulation 79 in a specific Annex for operational safety or incorporated into the requirements in Annex 7 and/or the main text
- OR introduction of a horizontal regulation for automated driving systems which includes operational safety requirements for level 3 systems, e.g. Cat B2, E.

An initial proposal for requirements for the assessment has been derived.

The following comments from ACSF IWG industry members were noted during the course of this work:

- The development process for operational safety can start 2+years before approval required. Involvement of technical service at such an early stage, (which, if regulation introduced, would be necessary to ensure requirements met), could likely delay development process.
- Most manufacturers (i.e. all conscientious ones) will perform a comprehensive assessment of operational safety as part of due diligence and as assurance against product liability issues.

5.3 Driver monitoring

5.3.1 Introduction

Section 4.4.3 identified certain issues with the currently proposed driver monitoring requirements ('hands-on detection' for Category B1 systems; 'driver activity detection' for Category B2 systems):

Hands-on detection, although addressing an important issue, applied as sole means of monitoring leaves room for misuse of Category B1 systems (e.g. phone-related activities with one hand). In the short term, this shall be evaluated and addressed by manufacturers during system development (HAZOP to cover reasonably foreseeable misuse), and this step of the OEM shall be checked by the technical service during the Annex 6 assessment if TRL's proposed changes to the Annex are implemented.

In the longer term, however, it should be considered whether additional, specific driver monitoring requirements in order to ensure a similar standard of misuse prevention between different systems are required. The current draft monitoring requirements for Category B2 systems are considered by TRL too unspecific and underdeveloped to ensure safe operation. Additional regulatory work will be required to develop appropriate requirements.

The following section provides technical information to facilitate a discussion on the way forward to defining additional, more specific driver monitoring requirements.

Different levels of autonomous driving present a range of human challenges in terms of the level of driver attention required to ensure safe and operation of a vehicle. The SAE J3016[11] levels of automation provide a six level taxonomy of driving automation, ranging from no automation to full automation. A key distinction in terms of driver involvement is between Level 2, where the human driver monitors the environment, and Level 3, where the automated driving system performs the *entire* driving task including monitoring the environment. The human driver performs a safety critical function in both SAE Levels 2 (Partial Automation) and 3 (Conditional Automation). For the purpose of this review human factors are considered in relation to vehicle operation at Levels 2 and 3.

The specific role required of the driver at each level has implications for the level of driver attention required to perform the desired task effectively. Driver monitoring technology can play a role to ensure that the driver's behaviour does not negatively impact the safe operation of the systems.

Technical requirements for driver monitoring systems that allow enforcement of the required behaviour for each ACSF category or SAE level would need to be developed by a working group involving experts in human factors and experts in the technology required. In TRL's view, the technical requirements for monitoring systems of varying levels should ideally be placed in a horizontal regulation that can be called upon by different

[11] http://standards.sae.org/j3016_201609/; or https://www2.unece.org/wiki/download/attachments/40009763/%28ITS_AD-10-08%29%20SAE_J3016_Taxonomy%20and%20Definitions%20for%20Terms%20Related%20to%20Driving%20Automation%20Systems.pdf?api=v2

regulations and can be updated and developed further independently of other technology domains related to automated driving, such as steering systems.

A first step to defining technical requirements is an understanding of:

- the range of human factors that can be measured to detect the extent to which a driver is paying sufficient attention to the driving task; and
- the current state of driver monitoring technologies that link human-derived data to in-car responses: sensor technologies used, measurement approaches, current system capabilities and limitations.

TRL therefore prepared the following review of current technology – available or in development – that also outlines the level of technology readiness of different solutions and their applicability in different autonomous driving contexts.

5.3.2 Driver monitoring technologies

Driver monitoring technology has developed to cover a range of driver states relevant to safe operation of a vehicle at SAE Levels 2 and 3. This includes; driver inattention, driver distraction and driver fatigue. Many of the technological solutions considered during this review seek to detect and mitigate against one or more of these three driver states.

At points in this review the phrase 'in the loop' is used to encompass the range of terms, and, where applicable, specific driver states are discussed. For example, the term "fatigue" is used to describe a state where a driver risks falling asleep at the wheel (in 'normal' driving conditions), but also includes less extreme levels of tiredness that may impact on a driver's ability to monitor the driving environment. The review has highlighted that a range of driver states are used interchangeably by manufacturers and stakeholders. For the purpose of this review we use the following definitions to describe two other driver states typically covered by driver monitoring technologies:

- Driver inattention: "…inattention occurs when the driver's allocation of resources to activities does not match the demands of activities required for the control of safety margins." (Engström *et al.*, 2013, p. 35).
- Driver distraction: "…where the driver allocates resources to a non-safety critical activity while the resources allocated to activities critical for safe driving do not match the demands of these activities." (Engström *et al.*, 2013, p. 35).

5.3.2.1 Proxy-based driver monitoring systems

An important technological development in the automotive sector has been the introduction of so-called "Driver Monitoring Systems". A range of motor manufacturers promote variants of these systems that seek to warn drivers of the potential of fatigue onset via audio beeps and visual messages. Products available on the market include: 'Tiredness Recognition Scheme' (SEAT), 'Fatigue Detection' (Volkswagen and Skoda), 'Driver Attention Alert' (Nissan), 'Driver Alert' Control (Volvo), 'Attention Assist' (Mercedes), and 'Driver Alert' (Ford).

For the purpose of this review it is important to highlight the limitations of this specific technology in the context of automated driving systems using two criteria. Firstly, the systems use driver inputs and vehicle movement characteristics as proxies (rather than directly measuring human characteristics) for driver fatigue, inattention and distraction. Examples include 'steering inputs', where steering inputs are compared to a baseline, and 'lane departures', where uneven progress along a carriageway (using lane marketing detection cameras) denotes potentially unsafe driver characteristics. In an automated driving context these characteristics are controlled by the ACSF rather than the driver, which prevents their use as sole driver monitoring device in this context. Secondly, related to the data input limitation, the functionality of the systems is thereby restricted by a number of factors; the systems are not designed to detect fatigue or distraction in the short term (i.e. on short journeys), they are also not suitable for urban environments, winding roads, sporty driving styles and poor road surfaces. It is possible that these systems may form part of a suite of in-car systems. However, more sophisticated technologies are under development that provides more reliable measurements of the three overlapping driver states of interest.

5.3.2.2 Non-proxy driver monitoring systems

Table 13 below provides an overview of the approaches that can be used to measure various driver states relevant to the SAE levels under consideration. These techniques measure the extent to which the driver is maintaining appropriate behaviours in respect to vehicle control. The table also outlines in which SAE level the technology has potential application.

Table 13: Summary of potential driver state measurement techniques

Approach / System	Technique	SAE Level Summary
Changes in eye movement		
Tracking of gaze	Video cameras capture images of the driver's face and a number of cues including eye gaze direction are used to infer driver states such as fatigue and gaze direction.	Level 2 and Level 3
Blink behaviour / Blink frequency	Measures the blink rate of a driver in real time via motion picture processing from which driver states are inferred.	Level 2 and Level 3
Eye closure	Automated detection of eye closure by using video imaging of the face then computation methods for locating the eyes and changes in intensity to determine whether eyes are open or closed.	Level 2 and Level 3
Physical measures		
Steering wheel torque	Measures the torque applied by an automated driving system to actuate the steering, which allows detection of whether or not the driver is holding the steering wheel (even if he is not actively steering).	Level 2 only
Steering wheel pressure	Sensors in the steering wheel detect pressure to determine whether the driver is holding the steering wheel.	Level 2 only
Facial Tracking / Head position	Uses infra-red light to locate pupils and detect head motion / position.	Level 2 and Level 3
Reaction time	Reactive tests, in which the driver must touch a device within a pre-specified time.	Level 2 and Level 3
Physiological measures		
ECG / Heart rate	Measurement of heart rate to infer driver states such as fatigue (via a seatbelt mechanism, head cap, ear piece, or pressure sensors in	Level 2 and Level 3

	the seat etc.).	

5.3.2.3 SAE Level 2 driver monitoring techniques

At SAE Level 2 the driver must monitor the driving environment and maintain full attention to the driving task but some physical aspects (e.g. steering and acceleration) can be controlled by the vehicle. Therefore, the level of attention required is not significantly different from a non-automated driving system.

Steering wheel torque or steering wheel pressure is a viable tool to ensure the driver maintains physical contact with the steering wheel, which is one of the prerequisites to enable a driver to react promptly to the driving environment. 'Hands-on' detection, reportedly via steering wheel torque measurement, is implemented in Tesla's Autopilot system.

Fatigue monitoring (via a range of systems) is a useful way to ensure that the driver is physically capable of performing the driving task. Similarly ensuring that the driver's attention is on the road environment (i.e. not looking away for significant periods of time) can be measured using eye gaze and head position technology.

5.3.2.4 SAE Level 3 driver monitoring techniques

At SAE Level 3 the driver is able to pass control to the vehicle but is responsible for monitoring the system, i.e. responding to requests to intervene as required by the vehicle system. Therefore many of same driver measurement techniques are applicable from Level 2 in a Level 3 context. However, in a Level 3 scenario a driver can perform certain short term tasks but cannot enter a state where he is not available to take back control within short notice, such as sleep. The implication from a driver monitoring perspective is that this could involve looking away from the road environment. As outlined in this review the technology exists to measure potential sleeping behaviour, ECG measurements and head position to infer whether a driver is asleep.

Driver gaze raises a different technical challenge in a Level 3 context to that of Level 2. Current monitoring systems are designed to detect glances of a frequency that may impact on safe operation of a vehicle in a non-automated driving context. Therefore systems would need to be adapted to be based on *acceptable gaze duration* in a SAE Level 3 scenario.

The review found an OEM that has incorporated this type of technology into a production vehicle. A similar system appears to be under development by Volvo (and other manufacturers) but as yet is not available to consumers. A brief summary of each system is provided below:

- **'Driver Monitoring System' (Lexus)**
  - Driver monitoring system used of part of A-PCS (Advanced Pre-Crash Safety) system.
  - Steering wheel mounted infrared sensor which monitors movement of driver's head and eyes.
  - Detects if the driver's head has turned to the side for a few seconds or if their eyes are closed
  - If the system detects the driver is distracted the A-PCS pre-crash alarm will be brought forward automatically.
  - **Current status:** Currently available on the Lexus GS 450h and LS 600h L models
  - **More information:** http://blog.lexus.co.uk/lexus-car-safety-monitoring-systems/#driverMonitoringSytem

- **'Driver State Estimation' (Volvo)**
  - Dashboard mounted infrared sensor
  - Detects which direction the driver is looking, how open the eyes are, as well as head position and angle

- Linked to other external system monitors that intervene if there is a risk of crashing e.g. lane keeping, collision warning with automatic braking, and adaptive cruise functions
- **Current status:** Under development
- **More information:** https://www.media.volvocars.com/global/en-gb/media/photos/140899/sensor-for-driver-state-estimation

5.3.3 System implementations

This section outlines driver monitoring systems identified in this review that measure one or a combination of factors described above. Table 14 to Table 17 provide a summary of the technologies available and other relevant information.

Table 14: Summary of driver monitoring technology (Eye Movement / Head Position)

Changes in Eye Movement / Head Position						
Company	**System**	**Driver State**	**Description**	**Output**	**Company Name / Further Info**	**Specification / Additional Information**
Denso	Driver's face angle, long-duration eye closure, drowsiness level and head position	Distraction and Fatigue ("Driver Status Monitor")	The device uses an integrated infrared camera and ECU (electronic control unit).	A warning will appear and/or the system might adjust vehicle features (e.g. mirrors)	https://www.denso.co.jp/ja/news/event/globalmotorshows/2013/files/NAIAS13_driver_status_monitor.pdf	"Highly adaptable to individual differences and changes in head pose or position Higher-performance tracking and accuracy under various vehicle and light conditions. New, DENSO-original technology – PEAC (Pose Estimation using A Camera)"
Seeing Machines – FOVIO (Tier 2 provider to Tier 1 supplier, Takata)	Eye and Face Tracking Technology	Distraction and Fatigue	Measures driver attention, fatigue and distraction by coupling image processing with scientific models of driver behaviour and physiology.	Various	http://www.fovio.com	"Seeing Machines has strategic relationships with Caterpillar, Electro-Motive Diesel, Boeing, Takata, Bosch, LG and Panasonic among others".
LumeWay: EyeAlert EA410	Blink rate / eye closure duration / head position	Distraction and Fatigue	The infrared product monitors eye closure rate and duration (Fatigue) and head position (Distraction)	Audible alert	LumeWay - http://lumeway.com/EA410.htm	Patented PERCLOS algorithms
Tobii Tech (Bespoke solutions offered)	Eyelid closure / eye gaze patterns	Distraction and Fatigue	Specific product information not available	Specific product information not available	Tobii Tech - http://www.tobii.com/tech/products/automotive/	Claimed to be appropriate for autonomous vehicle environments
Vigo	Head motion / blink rate	Fatigue	Infrared sensors to track blinks and head motion which are linked to algorithm patterns that detect drowsiness. The product is a bluetooth enabled ear piece. The	If drowsiness is detected, it stimulates the driver with a combination of vibrations, music, audio, a flashing light or phone	Vigo - http://www.wearvigo.com/	Charging: USB Talk time: 12 hours Standby time: 10 days Weight: 17 grams

Changes in Eye Movement / Head Position						
Company	**System**	**Driver State**	**Description**	**Output**	**Company Name / Further Info**	**Specification / Additional Information**
			product is also supported by an app	calls		
Continental Corporation (2013)	Eye and head movements	Distraction and Fatigue	Infrared interior cameras detect whether the driver is fatigued or distracted. This information is linked to an external driver assistance system	If a safety critical scenario is detected an LED light strip is activated	Continental - http://www.continental-corporation.com/www/pressportal_com_en/themes/press_releases/3_automotive_group/interior/press_releases/pr_2013_02_07_driver_focus_en.html	Vehicle manufacturer concept

Table 15: Summary of driver monitoring technology (Physiological Measures)

Physiological Measures (ECG)						
Company / Product Name	**Approach / System**	**Driver State**	**Description**	**Output**	**Company Name / Further Info**	**Specification / Additional Information**
Smartcap - Headwear cap	ECG Measurement	Fatigue	Real-time measurements of fatigue, based on direct physiological measurement via a headwear cap. Bluetooth wireless connection transmits data from the SmartCap to an in-cab display. The system is designed to prevent microsleeps and fatigue incidents	If specific fatigue criteria are met, visual and audio alarms are triggered (in-cab)	Smartcap - http://www.smartcaptech.com/our-product/	N/A
HPV/ fatigue detector (DFD-100B) - Seat belt mounted	ECG Measurement	Fatigue	Real-time measurements of fatigue, based on direct physiological measurement via a wireless seat belt mounted device	The device issues a warning beep whenever the driver's ECG / fatigue level drops below the set-up limit	Holux - http://www.holux.com/hcEN/en/products/products_spec.jsp?pno=413	Accuracy 90% False alarm rate Less than 1% Complies with IEC61000 & JAP WEPE electromagnetic compatibility of general industrial products

Table 16: Summary of driver monitoring technology (Physiological Measures)

Physical Measures – Reaction Time						
Company / Product Name	**Approach / System**	**Driver State**	**Description**	**Output**	**Company Name / Further Info**	**Specification / Additional Information**
Antisleep Pilot (ASP)	Fatigue Profile / Journey time / Accelerometer data / Reaction time	Fatigue	Drivers complete a short test to determine risk profile (via an iOS device). The ASP calculates fatigue level, and displays a real-time status. 26 different parameters, including personal risk profile, fatigue status, journey time, and input from a clock and accelerometer. It also maintains and measures driver alertness through occasional reactive tests, in which the driver must touch the device as soon as indicated.	Visible and audible signals alert of the need to take a break based on the risk parameters and the reaction test	https://www.youtube.com/watch?v=-nHSox9wYLc	N/A

Table 17: Summary of driver monitoring technology (Steering Wheel Pressure)

Physical Measures – Steering Wheel Pressure						
Company / Product Name	**Approach / System**	**Driver State**	**Description**	**Output**	**Further Info**	**Specification / Additional Information**
Hoffman and Krippner, (in cooperation with Guttersberg Consulting)	Steering wheel pressure	Fatigue	A microprocessor keeps track of the intensity, frequency and location of those shorts, and uses it to establish a typical driving pattern for the user.	When they deviate from it significantly, the car will then alert them to wake up and pull over.	http://newatlas.com/smart-steering-wheel-driver-drowsiness/38405/	Company concept
Panasonic	Steering wheel pressure	Fatigue	Steering Grip Sensing Technology	N/A	http://news.panasonic.com/global/topics/2014/28876.html	Company concept

5.3.4 Discussion

Going beyond simple hands-on detection, the most prominent technology in the field of driver monitoring appears to be centred on the use of infrared cameras that are hardwired into the vehicle. These systems detect a range of distraction / inattention / fatigue factors which have applicability in both SAE Levels 2 and 3. In terms of Level 3, they have the potential to ensure that the driver is 'available'' by detecting where and for how long the driver's head is turned away from the driving environment, and/or whether they are experiencing extreme levels of fatigue, micro-sleeps, or are asleep.

As shown above, a wide range of companies appear capable of equipping vehicles with this type of system if it were to be mandatory. Developments in the technology appear to be 'roll-out ready' following a range of incremental developments to overcome practical limitations e.g. functioning in low-light scenarios, detecting eye / head factors through sun glasses, glasses and contact lenses. Suppliers and automotive manufacturers (e.g. Lexus) have adopted variants of this technology and patented versions of the technology are available. Seeing Machines, for example, in conjunction with Takata claim to be supplying 15 automotive companies and have announced a number of strategic partnerships in the automotive sector (no further detailed information is publically available). Other Tier 1 and Tier 2 suppliers also have 'market-ready' versions of this technology. Obtaining technical information on product specifications can be difficult due to the commercially sensitive nature of the information.

ECG based systems are less prevalent in terms of market adoption and tend to be sold as stand-alone units via consumer channels. They are focused on fatigue factors only (whereas the systems above detect this and other factors such as inattention and distraction). The examples identified during this review appear to be 'portable' (i.e. not built into the car) and therefore need to be charged, putting an emphasis on the driver to maintain the battery levels. However, seat-based ECG measurement is feasible but not currently implemented.

Reaction time systems have potential in a SAE Level 3 environment to ensure a driver maintains a safe level of attention, but may present a nuisance to drivers in Level 3 contexts and a non-essential distraction in SAE Level 2 contexts or during 'normal' driving. Again, this solution appears to be sold via consumer channels rather than being incorporated in to vehicle systems. Similarly, steering based systems have potential in certain Level 2 contexts (i.e. to ensure a driver has control of the steering wheel) and are used in mass production vehicles already.

In summary, the technology exists to detect and react to the three main driver states considered during this review (fatigue, distraction and inattention). However, each of the systems would need to be tested in the *specific* scenario in an autonomous driving context. For example, in SAE Level 3, a driver could engage in other tasks. Further research would need to establish with a high degree of certainty whether eye or head position systems could detect, for example, between a driver looking down at a mobile phone and being asleep.

5.4 In-service safety performance monitoring

5.4.1 Background

With higher levels of automation, the complexity of decision and sensor fusion algorithms increases and the safety validation of automated driving systems becomes increasingly challenging – for both OEMs and type-approval authorities. This issue is particularly critical for systems where the driver is not expected to permanently monitor the driving environment (SAE Level 3 and above, ACSF Categories B2 and E) and can therefore not act as a safety net to overrule wrong decisions of the driving system.

The considerations laid out in preceding sections of this report clearly show that there is, as yet, no known mechanism or test that allows technical services to validate fully at the time of type-approval at a reasonable cost that the system will perform safely in all real-world scenarios that it may encounter. Instead the approach being developed is to check

a limited number of scenarios and aspects of the system development process, in particular the safety concept. It is therefore reasonable to assume an increasing potential for safety relevant issues in products which are not detected during type-approval in the future. To help counter this, it should be considered to strengthen safety monitoring mechanisms that act after the market deployment of automated driving systems. The following sections summarise the current status of US legislation (federal and California state law) in this regard and presents relevant considerations for the European system.

5.4.2 US federal requirements

The US Federal Automated Vehicles Policy[12] requires OEMs to have a process for collecting "*event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues.*" This applies to vehicles of SAE Level 3 and above during public road testing as well as after deployment to consumers.

For crash reconstruction purposes at least injurious collisions and collisions involving vehicle damage to an extent that the vehicle cannot be driven anymore have to be covered. Importantly, the US policy also acknowledges the fact that OEMs and regulators will need to develop new safety metrics to test and assess automated vehicles in the future. In order to create an evidence base for the development of such future metrics, OEMs should also collect data during non-collision incidents, such as near misses and edge cases (explicitly also in cases where the automated driving system contributed to a positive outcome). This data should be shared to enhance and extend safety benefits.

Under the US Early Warning Reporting program OEMs are required to provide NHTSA with information relating to injuries, fatalities, property damage claims, consumer complaints, warranty claims and field reports. This applies also to conventional cars where annual reports have to be filed. For automated vehicles, NHTSA urges OEMs to submit this information quarterly.

5.4.3 California state law

The Regulations of the California Department of Motor Vehicles (DMV) for autonomous vehicles are currently in draft stage, with the latest version published on 30th September 2016[13]. OEMs will require a permit from DMV for operating vehicles in autonomous mode (SAE Level 3 and above) in California. Permits will be issued in two stages:

- Testing on public roads
- Deployment to the public

During both of these stages OEMs are required to report, within 10 days, any accident "*originating from the operation of the autonomous vehicle on a public road that resulted in the damage of property or in bodily injury or death*". For investigation purposes the vehicles have to be fitted with an 'autonomous technology data recorder' (similar to UN R79 term DSSA) which has to record "*technical information about the status and operation of the vehicle's autonomous technology sensors for 30 seconds prior to a collision and at least 5 seconds after a collision or until the vehicle comes to a complete stop.*"

In addition, OEMs will be required to file annual reports on the safety performance of their vehicles during testing on public roads. The reports will contain information on any unplanned disengagements (i.e. deactivation caused by a failure or by the test driver

[12] US Federal Automated Vehicles Policy – I. Vehicle Performance Guidance for Automated Vehicles, E. Cross-Cutting Areas of Guidance, 1. Data Recording and Sharing
http://www.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf

[13] California Express Terms, Title 13, Title 13, Division 1, Chapter 1, Article 3.7 – Autonomous Vehicles
https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/auto

intervening). The following data shall be summarised in the annual reports for each month:

"(A) The total number of autonomous mode disengagements and the circumstances or testing conditions at the time of the disengagements including:

(i) The location: interstate, freeway, highway, rural road, street, or parking facility.

(ii) A description of the facts causing the disengagements, including: weather conditions, road surface conditions, construction, emergencies, accidents or collisions, and whether the disengagement was the result of a planned test of the autonomous technology.

(B) The total number of miles each autonomous vehicle tested in autonomous mode on public roads each month.

(C) The period of time elapsed from when the autonomous vehicle test driver was alerted of the technology failure and the driver assumed manual control of the vehicle." (§227.46. Reporting Disengagement of Autonomous Mode)

Annual disengagement reports filed by Google, Tesla, Bosch, etc. are available for download from DMV14. These reports show a wide variation in length and depth of problem description.

Before deployment to the public, the OEM must certify to DMV that the causes of any unplanned disengagements have been evaluated and resolved. DMV may suspend or revoke a permit for various reasons, including that "*the department determines the manufacturer's vehicles are not safe for the public's operation […] based upon the performance of the vehicles."*

5.4.4 Considerations for the European type-approval and recall system

Based on the General Product Safety Directive (Directive 2001/95/EC), a manufacturer selling cars on the European market is required to inform the competent authority of any issues they have with the safety of their products. Additionally, under the Framework Directive (Directive 2007/46/EC), OEMs have to notify their type-approval authority of any safety recalls on an approved product.

Algorithmic faults of automated driving systems might not be identified at type-approval stage and could, in the field, arguably lead to a high number of collisions in a short space of time or a number of safety incidents becoming apparent only occasionally in a wide variety of different incidents. In order to ensure that OEMs are in a position – and under obligation – to initiate a recall soon after problems first appear in the field, they could be required to collect data on and monitor the in-service safety performance of their automated vehicles of SAE Level 3 and above. Data collection requirements for a vehicle model or software version could be limited to a certain time after deployment.

It should be noted that some of these data may be 'personal' or 'sensitive' data and be subject to the European data protection rules (Regulation and Directive). An agreement may need to be established between the customer and the OEM to allow collection and subsequent processing, and clarify the question of data ownership. While data collection for the entire new-vehicle fleet equipped with a specific system would give the best representation of in-service safety performance, it should be noted that a random sample large enough to draw significant statistical conclusions could also be sufficient. The latter could still be achieved if a proportion of customers are not willing to agree to a voluntary data collection agreement with the OEM. An in-depth legal analysis of the implications of data protection rules and questions of data ownership is advised if this concept should be developed further.

Data acquisition for analysis is perceivable in different ways:

[14] https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/disengagement_report

- Ad-hoc collection by OEM (over-the-air transmission, shortly after incidents happen)
- Intermittent collection by OEM (data download, e.g. when vehicles return to a dealership for service or repair)

In order to be effective at preventing collisions, the data collected should also cover non-collision incidents indicative of safety issues, such as unplanned disengagements of the automated driving system leading to minimum risk manoeuvre, emergency hand overs to the driver, sensor discrepancies that cannot be resolved, or near miss incidents. OEMs would be in the best position to define the exact data required to assess the safety of their systems and to perform the analysis for safety issues.

Additionally, a requirement to file reports of the safety monitoring to the type-approval authorities or the Commission could provide a knowledge and evidence base that would support the development of new safety metrics for effective future legislation. The Commission could also use these reports for market surveillance purposes in their potential future role under the proposed type-approval regulation15.

5.5 Summary and discussion of way forward

Review of the current ACSF IWG proposal highlighted four major issues. Work reported in this section developed proposals to address each of these issues as follows:

1. Inconsistent interpretation and application of CEL Annex (Annex 6)
    - Currently, the Annex 6 assessment process is not applied in a consistent manner across technical services. Current 'best practice' application has been identified and amendments to Annex 6 proposed to implement it. The elements of best practice identified for inclusion within Annex 6 were:
        - Early involvement of the technical service in the development process to ensure good understanding of safety approach and concept
        - 'Audit' of confidential documentation provided, usually performed on site at OEM or if necessary supplier. Audit should include:
            - Inspection of safety approach at both concept (e.g. HAZOP) and system level (e.g. FMEA, FTA). Check existence of documents/files, their history and (to a certain extent) the content of the documents/files.
                - Note: safety approach at concept level should include consideration of:
                    - Risks driven by interaction of CEL system with other vehicle systems, e.g. effect of LKA on AEB and/or ACC
                    - Risks driven by reasonably foreseeable misuse by driver
    - Traceability of work performed by technical service to level that would allow work to be repeated, e.g. versions of documents inspected are coded and listed
    - Resistance to environmental influence, type and scope of tests on climate and mechanical resistance and electromagnetic compatibility should be inspected
    - Possibly, include report template to assure all aspects addressed; an example of a template produced by the German approval authority KBA template is available publicly for information
2. Safety under all real-world scenarios (operational safety)
    - For lower category systems (CSF and B1) the current ACSF IWG proposal requires 'hands-on' operation. Physical contact with the steering wheel is an important prerequisite to enable a driver to react promptly to the driving environment. Enforcement of steering wheel contact will also give

[15] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016PC0031

conscientious drivers a strong indication of the expectation put on them to permanently remain in control of the vehicle. (However, in TRL's view, hands-on detection alone may not prevent all foreseeable misuse: see related recommendations on driver monitoring below). On this basis, in the short term, TRL recommend that no additional requirements for operational safety are necessary for lower category systems (CSF and B1). However, in the longer term additional requirements for driver monitoring should be considered, especially if a regulation dedicated to driver monitoring is developed.

- For higher category systems (B2 and E), the current proposal permits 'hands-off' operation and also allows up to about three minutes in which the driver may be 'out of the loop' and may not be monitoring the environment. Therefore, for this period the system must be capable of controlling the vehicle. Hence, TRL recommend that requirements similar to those for a level 3 system should be imposed, i.e. a comprehensive assessment to assure safe operation in the full range of real-world conditions which may occur in the operational design domain (ODD) is required. An initial list of requirements has been developed.
- These requirements could be implemented within Regulation 79 or more logically in a new horizontal regulation for automated vehicles.

3. Driver monitoring
   - TRL's review of the draft working documents identified some issues with the currently included driver monitoring requirements ('hands-on detection' for Category B1 systems; 'driver activity detection' for Category B2 systems):
   - Hands-on detection alone leaves room for potential misuse of Category B1 systems (e.g. phone-related activities with one hand). In the short term, this should be evaluated and addressed by manufacturers during system development (HAZOP to cover foreseeable misuse), and this step of the OEM should be checked by the technical service during the Annex 6 assessment if TRL's proposed changes to the Annex are implemented.
   - In the long term, however, it should be considered to develop additional, specific driver monitoring requirements in order to ensure a similar standard of misuse prevention between different systems. The current draft monitoring requirements for Category B2 systems are considered by TRL too unspecific and underdeveloped to ensure safe operation. Additional regulatory work will be required to develop appropriate requirements. These should ideally be placed into a horizontal regulation that can be called upon by different regulations and can be updated and developed further independently of other technology domains related to automated driving, such as steering systems.
   - TRL's technology review of driver monitoring technologies and system implementations found that the technology exists to detect and react to the three main driver states considered during this review (fatigue, distraction and inattention). Going beyond simple hands-on detection, the most prominent technology appears to be centred on the use of driver-facing infrared cameras.
   - Each of the systems would need to be tested in the specific scenario in an autonomous driving context. For example, in SAE Level 3, a driver could engage in other tasks. Further research would need to establish with a high degree of certainty whether eye or head position systems could detect, for example, between a driver looking down at a mobile phone and being asleep.
4. In-service safety performance
   - For automated vehicles SAE level 3 and above, the US 'Federal Automated Vehicles Policy' will require OEMs to collect, '*event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues'.* California state law also requires reporting of accidents, incidents, etc. for these vehicles. It is recommended that

implementation of a similar system coupled with the recall system in the EU coupled should be considered. Such a system could oblige OEMs to collect safety data so that they are in a position – and under obligation (according to Article 32 of the framework Directive) – to initiate a recall if safety problems were identified in the field.

- For the way forward, it is interesting to consider the strategy for implementation of the regulatory measures proposed above, especially for higher category systems (B2 and E). For these systems there is, as yet, no known mechanism or test that allows technical services to validate fully at the time of type-approval at a reasonable cost that the system will perform safely in all real-world scenarios that it may encounter. Instead the approach being developed is to check a limited number of scenarios and aspects of the system development process, in particular the safety concept. It is therefore reasonable to assume an increasing potential for safety relevant issues in products which are not detected during type-approval in the future. To help counter this, clarification will be needed that manufacturers will bear the full responsibility for their products (e.g. by a self-declaration on the safety of their product) and/or in-service safety performance monitoring coupled with recall action to address any safety issues identified is could be implemented.
- From a strategy point of view, the aim is to ensure safe performance of ACSF in all real-world conditions. This can be achieved by adding more scrutiny up-front (e.g. requirements for operational safety) and/or ensuring that safety issues in real-world use are detected and resolved early (e.g. in-service safety performance). The interesting question in terms of strategy is should both approaches be used, and if so, what balance of the two approaches should be used.
- At this stage it is not possible to answer this question definitely. However, on the basis that it is proposed to use both approaches in the US Federal Automated Vehicles Policy, it would appear sensible that measures should be put in place in UN Regulation to enable the use of the three approaches (enhanced requirements for operational safety checked by authorities at type-approval level, self-declaration by the manufacturer on some design aspects and proactive in-use safety monitoring. From the point of view of amendments to Regulation 79, this would entail introducing requirements for the collection of, "*event, incident, and crash data, for the purposes of recording the occurrence of malfunctions, degradations, or failures in a way that can be used to establish the cause of any such issues*", for higher category ACSF systems (i.e. B2, E). In the current ACSF IWG proposal (Section 5.6.1.8.) there is only a requirement for collection of data 'after a road accident'. It is recommended that these requirements are expanded as detailed in Section 4.3, Table 11, to include collection of data for events, incidents and road accidents sufficient for use to establish the cause of any such issues and any related system defects. It should be noted that some of these data may be subject to the European data protection rules (Regulation and Directive) and therefore an agreement may need to be established between the customer and the OEM to allow collection and subsequent processing, and clarify the question of data ownership.

6 Task 5: Draft EU type-approval guidelines for OTA updates

The objective of this task was to provide options for type-approval arrangements that could apply to vehicles undergoing OTA updates after gaining type-approval where the updates materially change the characteristics or performance of the vehicle or its safety systems.

To achieve this objective the following activities were undertaken:

- Document the current update process for updates to safety system performance and operation.
- Review this to identify where steps are (or can be) linked to regulatory controls
- Describe how the process could be influenced by OTA updates.

6.1 Current update process

6.1.1 Updates to vehicles pre-production

The main reason of why an Original Equipment Manufacturer (OEM) may wish to make updates to a vehicle's systems which affect a vehicle's type-approval are to improve the vehicle performance for a model upgrade (face-lift). Examples are:

- Change bonnet stiffeners to provide greater pedestrian safety, possibly to improve the Euro NCAP rating – This type of update is likely to be done for pre-production (pre-registered) vehicles only.
- Change the engine ECU mapping to improve engine performance and / or emissions – This type of update could be done for both pre-production and post-production (new and registered vehicles), but would generally only be performed for pre-production vehicles.

The framework Directive 2007/46/EC contains a number of articles related to updates of vehicle pre-production which affect type-approval in particular articles 4 and 5 (obligations for the manufacturers and Member States) as well as Article 13 to 16 (procedure for amendments to EC type-approval).

In general the procedure for vehicles pre-production is:

1) The OEM identifies the components / system they wish to change and provides reason for the change and information on which directive/legislation they think is affected by the change.

2) The OEM makes contact with a type-approval authority (for the UK this is the Vehicle Certification Agency), with information on the changes to be made and evidence of the impact of the changes. The OEM may present in house-data as evidence of the impact of the change.

3) The Type-approval authority reviews the changes in light of initial worst case agreements for that vehicle type, and assesses if the new proposals require new worst casing and testing, or if the changes are already covered by the worst case agreement currently in place.

3a) If changes comply with original worst casing then the approval certificate for the component that is changed is extended and issued with a new test report which refers to the manufacturer's documentation (including in-house data) and indicates that the worst case does not require a change.

3b) If changes are deemed to require a new worst case, then the component must be retested in accordance with the directive/legislation in question and a new approval certificate is issued with a copy of a test report and the manufacturer's documentation.

Notes:

- Only new vehicles would be covered by the extension. Vehicles that are already on the road would be covered by the previous approval unless the changes are made for the purposes of a recall – see Section 6.1.2 below. This applies to both steps 3a and 3b.

6.1.2 Updates to vehicles post-production

Updates on post production vehicles are usually done to retrofit/modify a vehicle or to correct a vehicle defect through a recall.

Post-production non-recall related updates on used vehicles are currently not regulated as such in the EU type-approval or UNECE legislation. Many EU Member States require the vehicle owner to keep the vehicle in compliance with its approval and therefore any major change to the vehicle may require the vehicle to undergo a new approval ("individual approval"). Other Member States are more flexible with modified vehicles and may just require a periodical technical inspection. The EU type-approval legislation or UNECE Regulations can provide some degree of harmonization in the national rules. Typical examples are CNG and LPG retrofitting of vehicles or replacement parts. For instance, UN Regulation 115 on the retrofitting of LPG/CNG guarantees a certain level of safety and emissions for the parts approved under this Regulation but the fitting of those parts is generally checked through a national individual approval. Similarly, UN Regulation 90 on replacement brake discs and pads certifies a certain level of quality for those parts, but the correct fitting of these parts is purely the responsibility of the owner/repairer.

Regarding vehicle defects, the Recall procedure post production for dangerous products within the EU is governed by the General Product Safety Directive (GPSD) 2001/95/EC. Article 6 of this Directive requires that all member states establish or nominate authorities to monitor the compliance of products with the general safety requirements and arrange for such authorities to have and use the necessary powers to take appropriate measures incumbent upon them under the GPSD. As an example, in the UK, the Driver and Vehicle Standards Agency (DVSA) is the nominated national authority for automotive safety issues. DVSA has a specific team, the Vehicle Safety Branch (VSB), responsible for this work (DVSA, 2007). Typical defect recalls are to correct a problem related to the safety of the vehicle. Examples of safety related recalls include:

- Steering components that break suddenly causing partial or complete loss of vehicle control.
- Problems with fuel system components, particularly in their susceptibility to crash damage, that result in leakage of fuel and possibly cause vehicle fires.
- Air bags that deploy under conditions for which they are not intended to deploy.
- Accelerator controls that may break or stick.
- Wheels that crack or break, resulting in loss of vehicle control.
- Engine cooling fan blades that break unexpectedly causing injury to persons working on a vehicle.
- Windscreen wiper assemblies that fail to operate properly.
- Seats and/or seat backs that fail unexpectedly during normal use.
- Critical vehicle components that break, fall apart, or separate from the vehicle, causing potential loss of vehicle control or injury to persons inside or outside the vehicle.
- Wiring system problems that result in a fire or loss of lighting.
- Car ramps or jacks that may collapse and cause injury to someone working on a vehicle.

The process for recall consists of the following steps, not necessarily in order:

1. The OEM informs nominated national authority of their intent to perform a recall or the national authority requires the OEM to carry out a recall:

2. The OEM gathers information for vehicles affected which includes

- Make and model
- Vehicle keeper details
- Build dates
- VIN numbers
- **Issue/concern identified**
- **Possible consequences**
- The repair
- Numbers of vehicles/products involved and which countries (EU member states) they are in.
- Parts information
- Relevant type-approval number(s)

3. The OEM informs type-approval authority of recall (required by Article 32 of the framework Directive 2007/46/EC).

   As for updates to vehicles pre-production (section above), the OEM liaises with the type-approval authority to check if the repair updates will be covered by current approvals and if not update approvals as appropriate.

   Note that in the UK, the type-approval number is used as the reference number for the recall.

4. The nominated national authority informs RAPEX of recall, so that all the member states are notified of the recall. RAPEX is a European Union initiative under the GPSD Directive 2001/95/EC in order to collaborate and share information about serious issues that affect products sold in member states. A network of enforcement authorities within Europe supply information to the Community Rapid Alert System (RAPEX).

   In general, all consumer product recalls that affect European Union member states Norway, Iceland and Liechtenstein should be reported to RAPEX.

5. The OEM notifies the registered vehicle keepers and dealers of the recall and the action they should take, which usually involves taking the vehicle to a dealer to perform the updates necessary. Notification of the vehicle keepers is usually by letter which is mailed but other means of communication can be used as well such as:

   - National and local press articles
   - TV and radio advertising
   - Press statements
   - Posters displayed in relevant outlets, garages and community facilities
   - Official website entry
   - Owner's club websites
   - Text messaging
   - Email
   - Telephone call

6. Perform and monitor recall

   The OEM monitors the response rate to the recall and reports it regularly to the nominated national authority. Additional mailing may be needed to increase response rates. In certain cases incentives may be offered to help increase the recall response rate. Recalls may be closed for reporting purposes when there has been no further growth in the response rate for a significant time. However, it should be noted that as far as the producer and/or distributor is concerned the safety recall stays open indefinitely and a customer's recall work should be

undertaken free of charge, regardless of the length of time that has elapsed after the notification letter.

6.1.2.1 Additional recall procedure details for vehicle software updates

Safety related recalls can require vehicle software updates which affect the vehicle's ECUs. These ECUs are located throughout the body of a vehicle and require special tools and procedures to communicate with and successfully achieve a reliable update. Therefore these recall updates are usually implemented in a controlled environment by a Dealer, to ensure they are done correctly.

The following is typical of the update procedure at the dealers:

1. The OEM issues a recall notice (or new software release) to dealers and customers.
2. The OEM sends the latest software to the dealer, for example secure download or on a CD.
3. The customer is informed of update and takes vehicle to the dealer.
4. A technician connects the reprogramming tool to the in-vehicle bus and updates/flashes the faulty ECU with the content/update provided by the OEM.
5. The technician ensures update successful by using the diagnostic test services before and after the update.
6. Customer is contacted to pick up vehicle.
7. Dealer charges the OEM for labour costs.

For non-safety related recalls, usually radio/infotainment services, software updates are sometimes implemented by the customer. In this case, the customer either receives a CD with the latest software directly from the OEM or has to manually download the software onto a USB drive. To successfully update the radio/infotainment system, it usually requires the user from 30 minutes to several hours beginning with the download procedure and ending with the update confirmation. This update method gives customers the benefit of updating the radio/infotainment system at their own convenience. However, this method is not particularly good because, generally, not only is the procedure unintuitive, but there is also an additional security risk of having the software in the hands of many customers. This can increase the possibility of reverse engineering and the upload of a hacked version of the file to the internet.

6.2 Potential influence and status of Over-the-Air (OTA) updates on recall procedure.

Over-the-air (OTA) software / firmware updates have the potential to offer a large benefit to the automotive industry due to their capacity to reduce warranty costs, potentially increase overall completion rates for software related recalls, improve customer satisfaction by eliminating trips to the dealership for software upgrades or fixes, and provide the ability to upgrade functionality and add features to automotive infotainment systems over a vehicle’s lifetime.

OTA software update technology could ultimately help guarantee both fast accelerated Time-to-Market and Time-to-Road, enabling fully automated update flashing, comprehensive version control, and simplified, generic hardware-driven software localisation.

However, if OTA updates are used to upgrade functionality, especially if the system update provides a new function subject to type-approval which was not initially type-approved, or functionality is upgraded in a manner that has an impact on type-approval values (engine power, CO2 emission, pollutant emission level, etc.) used for purposes such as taxation or the implementation of transport policies such as low emission zones, this may cause problems in that the registration details for the vehicle may need to be altered also. It may also potentially create safety issues if this update relates to the safety critical functions.

Over-the-air updating is already in use among some vehicle OEMs as an alternative to performing the software updates using a vehicle workshop system, (e.g. Mercedes-Benz

for non-safety related (infotainment apps) updates, using the *mbrace* embedded telematics system and Tesla for ADAS functionality updates).

A study performed for the WP29. ITS/AD working group (WG) (Sena Consulting, 2016) lists the following technical conditions that an OTA software update standard should meet to be useful and acceptable:

- It must address the entire end-to-end life-cycle processes for the vehicle and its electronics systems.
- It must use the most secure and cost-effective method for performing the updates. It is not simply a matter of defining a protocol or delivering confirmation of completion.
- The standard must address the design of the embedded system, including how the system is activated and provisioned with its contact logic, and how it interfaces with the mobile network or other networks, such as Wi-Fi.
- It must address what to do when a system should perform as if it has been de-activated (e.g. if the customer does not wish to have an actively connected vehicle).
- The design of the system must also conform to the regulations of privacy that are in effect in the jurisdiction where the vehicle is located when the update is performed.
- Above all, the updating process should be done in complete alignment with the safety and environmental regulations that are in effect in each of the jurisdictions where the vehicles are sold.

The study also summarises operational and functional requirements for secure OTA vehicle software updates. Note that the study assumes that appropriate security is present but does not discuss how it may be realised. Operational requirements are summarised by dividing into the following six phases:

1. Prepare the update.

2. Obtain regulatory approvals for the update, if required.

3. Obtain the necessary permissions to perform the update from the authorized driver or registered owner.

4. Manage the update end-to-end.

5. Confirm receipt and proper functioning of the update.

6. Perform administrative tasks.

Each of these phases must be considered in relation to the Conditions of the vehicle (location and status of connectivity), the presence of the Authorized Driver and the process for an attempt to Re-deliver the update if the primary process fails. The nature of the update must also be considered, i.e. recall update, non-recall operation updates, performance improvements updates or security risk correction action updates.

Each OEM providing OTA updates should have a group that is designated to manage the end-to-end firmware and software over-the-air update delivery process.

The study summarises functional requirements by the nature of the update and the conditions of the vehicle (location and status of connectivity). Obviously the vehicle can only be updated when it is not in use, it has good connectivity and has sufficient power for the electrics. Figure 11 shows the current process for recall for a software / firmware update. Figure 13 shows the same process using OTA. The main differences are caused by the additional actions needed to obtain the necessary permissions from the authorized driver or registered owner and to confirm receipt and proper functioning of the update and if not take appropriate action, i.e. take ECU back to state prior to start of failed update. For completeness, Figure 13 shows the potential process for an OTA firmware update for a safety recall for car pre-delivery at dealer.

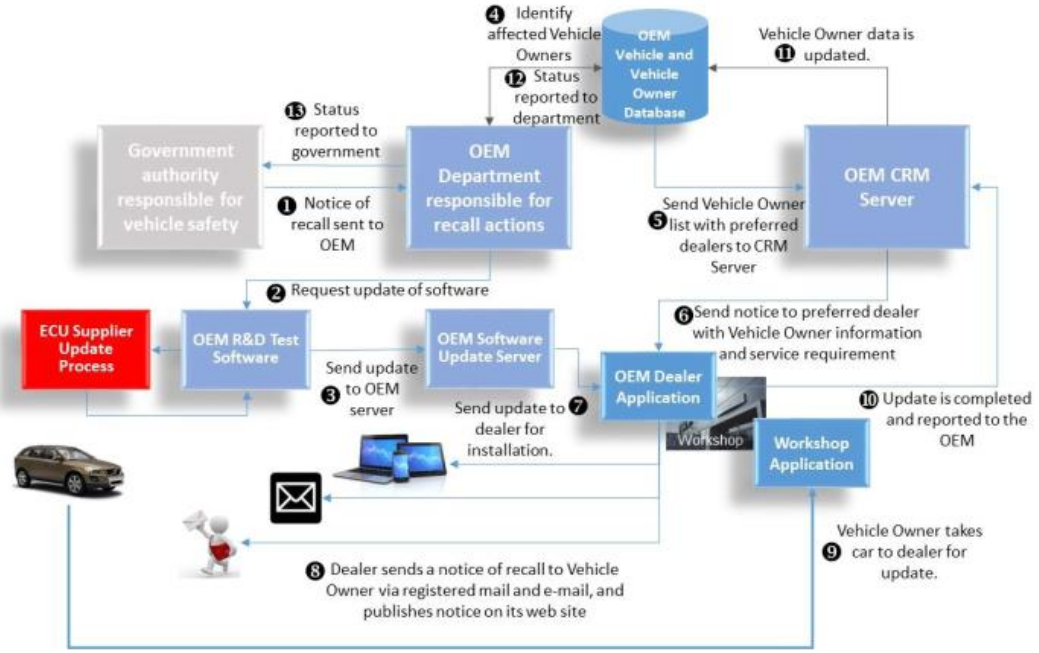

Figure 11: Current process for safety recall (Sena Consulting, 2016).

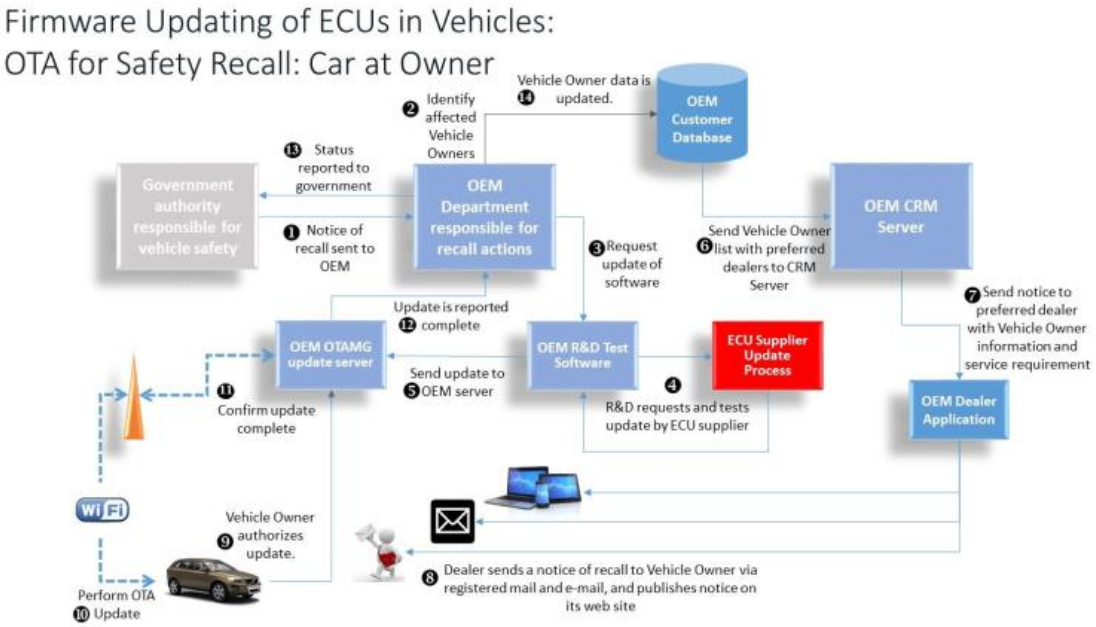

Figure 12: Potential process for an OTA firmware update for a safety recall for car post-delivery at owner's residence (Sena Consulting, 2016).

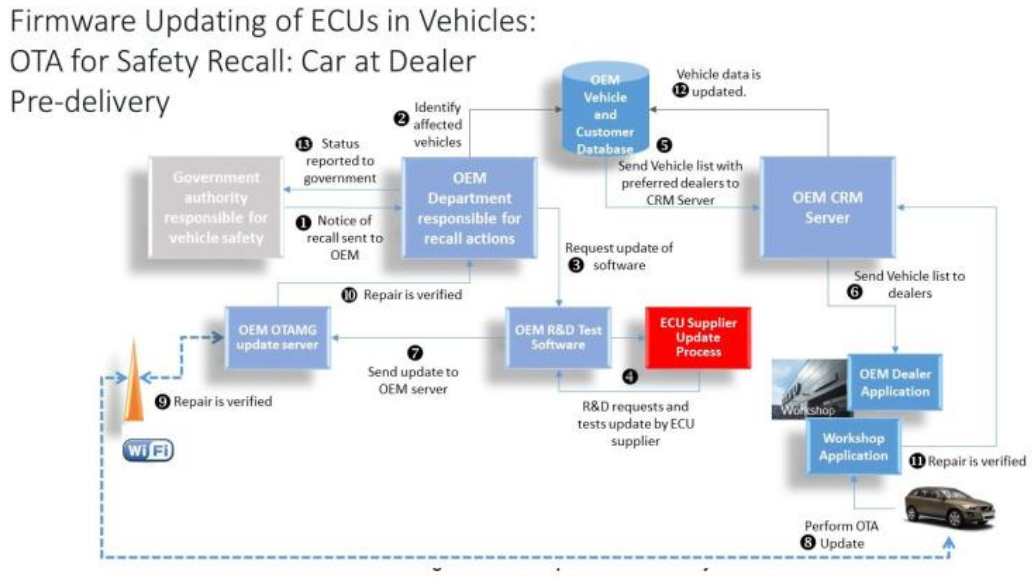

Figure 13: Potential process for an OTA firmware update for a safety recall for car pre-delivery at dealer (Sena Consulting, 2016).

Overall, the study focuses on the processes for making the update from a technical point of views, but does not address some of the administrative problems, such that some changes in functionality may need re-approval and /or changes to the registration of the vehicle.

This type of issue is highlighted in a more recent ITS/AD IWG document called 'Relations between type-approval and post-sale OTA software updates for automotive related systems'[16]. This document describes briefly the state of the art of software updates, that these types of updates can substantially and quickly alter a vehicle's performance capabilities after its manufacture and initial certification or type-approval. It then notes that the statute underlying FMVSS and regulatory frameworks for type-approvals is for manufacturer certification or approval of a vehicle prior to its manufacture and also that type-approvals are the administrative basis for a vehicle registration. It suggests an idea for how to deal with OTA software updates within the TA system assuming that the update is type-approval relevant. The idea is to treat the OTA software update as if it was both a model update in its production life cycle and as if the upgrade would correspond to a replacement part or retrofit. Contracting Parties may decide that a vehicle or system receiving an update shall be subject to approval, provided that the update concerns a matter of relevance for type-approval extension or revision. Process wise, the approval extension or revision shall be granted before the software update takes place and would be both an extension for products with the new software leaving the production line and a "retrofit" approval for the vehicles already in use and benefiting from the update.

Problems with this idea arise if the update cannot be covered by an approval extension or revision, especially if the system update provides a new function subject to type-approval, which was not initially type-approved. For automated vehicles, this problem is recognised in NHTSA's Federal Automated Vehicles Policy (NHTSA, 2016). The policy states that re-certification (i.e. equivalent to re-approval for the EU) may be needed, and also the development of additional measures and tools to ensure that consumers are adequately educated about the software update. Also, if performing OTA updates as corrective actions against safety and (cyber) security risks, the emergency character of

[16] Document No. ITS/AD-10-13. https://www2.unece.org/wiki/download/attachments/40009763/%28ITS_AD-10-13%29%20Working%20Paper%20on%20OTA.pdf?api=v2

these updates raises the question whether or not authority involvement should precede the deployments because it would likely increase the application timescale.

6.2.1.1 Security

Cyber-security for vehicles in general and for OTA updates is recognised as an area which requires much improvement. There are currently no common standards or industry practices for how an on-board system should be designed to achieve the highest level of security for both safety and security services and the broader range of infotainment services. What is known by all OEMs is that security of their on-board connected vehicle systems can be breached, and the consequences can be dire.

The European Union Agency for Network and Information Security (ENISA) is currently performing work on cybersecurity for smart cars. They will identify smart car and vehicle manufacturers and operators and will take stock of cybersecurity risks and challenges introduced by the use of the IoT. As part of this work, ENISA will identify all relevant public and private stakeholders, engage them in working groups and jointly take stock of and analyse the current situation in terms of cybersecurity and resilience giving emphasis on communication security. The Agency will also identify EU and national-funded projects in the area of IoT and M2M communication, liaise with them, analyse their findings and deliverables, and further engage them in corresponding expert groups. Special emphasis will be given to the resilience and robustness of such smart critical information. They will then develop good practices for private and public stakeholders.

The WP29. ITS/AD working group is currently discussing cyber-security and developing guidelines on measures to ensure cybersecurity and data protection of connected vehicles and vehicles with automated driving technologies. At present, drafting of the guidelines is ongoing, so only initial drafts are available (WP29. ITS/AD working group, 2016).

6.3 Discussion and proposed way forward

OTA software / firmware updates have the potential to offer large benefits to the automotive industry due their capacity make software updates easier and thus potentially increase customer satisfaction and completion rates, in particular for recalls linked to cyber security issues.

However, if OTA updates are used to upgrade functionality, especially if the system update provides a new function subject to type-approval which was not initially type-approved, this may cause safety or emissions problems and make the vehicle not compliant with its initial type-approval and its registration certificate.

From a regulatory point of view, OTA updates of pre-registered/production vehicles affecting approved functions could follow the current practice for a type-approval update. Manufacturers would have to inform the type-approval authorities about changes that affect a type-approved system (i.e. steering function in the case of R79) and the type-approval authorities would have to decide if such changes should be considered as a revision/extension or as a new type-approval. For Regulation 79, this may require the change of the type definition as today it does not include the category of ACSF with which the steering function is equipped.

Post-registration/production OTA updates on registered vehicles create more challenges regarding harmonization, because modifications to registered vehicles are covered by national legislation and not EU rules. These challenges could lead to a different legal treatment of OTA updates across the EU. In order to ensure a coherent approach around the EU and decrease the burden on manufacturers and vehicle owners, the EU type-approval framework could be extended to manage software updates that could affect approved systems of used vehicles in a similar way as there are today UN regulations on the retrofitting of LPG/CNG vehicles or for replacement parts. Relevant software updates could be validated by type-approval authorities (this may require new testing, e.g. in case of change of functions). Then the update could be deployed by manufacturer entirely under the manufacturer's responsibility and/or in combination with an individual approval/periodic technical inspection (PTI) depending on the scope of the update.

For updates deployed purely under the manufacturer's control, the question of responsibility should be clarified because today under most of national rules, it is the vehicle owner who is responsible for maintaining the vehicle in compliance with the relevant legislation. It may also be difficult to check remotely that the updated vehicles still meet the approval requirements. This may lean in favour of a solution of limiting the OTA updates to non-critical functions and require a physical inspection (by the manufacturer, authorities) for critical functions. Software updates not impacting the type-approved functions could be left out from the type-approval framework.

Software / firmware versions of safety and environmental systems could also be checked at PTI to ensure that vehicle has received all appropriate updates and has not been tampered with. The Implementing Act for Directive 2014/45/EU may offer an opportunity to implement this, if appropriate information was to be included within the technical information that manufacturers are obliged to supply to PTI authorities for inspection purposes. Discussions, led by the European Commission's DG Move, on what to include in the Implementing Act are ongoing at present. However, it should be recalled that the first PTI only occurs after a number years (after 4 years for cars in many member states).

Cyber-security is still a major issue and much work is being performed on it at present, for example the guidelines being prepared by the WP.29 ITS/AD working group. Until security issues are resolved, it will probably not be possible to perform OTA updates for safety and/or environmental vehicle systems.

7 References

Adaptive (2016). *Adaptive project deliverables and papers.*, viewed August 2016 Available from: https://www.adaptive-ip.eu/index.php/deliverables_papers.html.

Adaptive (2016). *Adaptive project website.*, viewed August 2016 Available from: https://www.adaptive-ip.eu/.

DVSA (2007). *MAnufacturer's guide to recalls in the UK Automotive sector.*, viewed Sept 2016 Available from: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/302389/manufacturers-guide-to-recalls-in-the-uk-automotive-sector.pdf.

Engström J, Monk C, Hanowski R, Horrey W, Lee J, McGehee D and Yang C (2013). *A conceptual framework and taxonomy for understanding and categorizing driver inattention. Brussels, Belgium: European Commission*.

Merat N, Jamson A, Lai F, Daly M and Carsten O (2014). Transition to manual: Driver behaviour when resuming control from a highly automated vehicle. *Transportation Research Part F: Traffic Psychology and Behaviour, 27*(B), 274-282. doi:http://dx.doi.org/10.1016/j.trf.2014.09.005.

NHTSA (2016). *Federal Automated Vehicles Policy.*, viewed Sept 2016 Available from: https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

OICA (2016). *Boundaries CSF-ACSF, New definition and requirements, Presentation at 7th ACSF meeting, ACSF-07-19.*, OICA, London, viewed August 2016 Available from: https://www2.unece.org/wiki/download/attachments/30540137/ACSF-07-19%20-%20%28OICA%29%20-%20Boundaries%20CSF%20-%20ACSF.pdf?api=v2.

Response-3 (2009). *Code of practice for the design and evaluation of ADAS.*, viewed August 2016 Available from: https://www.acea.be/uploads/publications/20090831_Code_of_Practice_ADAS.pdf.

Royce W (1970). Managing the development of large software systems. *IEEE*.

Sena Consulting (2016). *Secure Over-the-Air vehicle software updates.*, viewed August 2016 Available from: https://www2.unece.org/wiki/download/attachments/29884809/%28ITS-AD_08-09%29%20Secure%20Over-the-Air%20Vehicle%20Software%20Updates%20-%20Operational%20and%20Functional%20Requirements%20%2820160224%29.pdf?api=v2.

Van Eikema Hommes QD (2016). *Assessment of safety systems for automotive electronic control systems.*, viewed August 2016 Available from: http://www.nhtsa.gov/DOT/NHTSA/NVS/Crash Avoidance/Technical Publications/2016/812285_ElectronicsReliabilityReport.pdf.

WP29. ITS/AD working group (2016). *Preliminary draft proposal for guidelines on measures ensuring cybersecurity and data protection of connected vehicles with automated driving technologies.*, viewed August 2016 Available from: https://www2.unece.org/wiki/download/attachments/34701368/%28ITS_AD-09-03%29%20Revised%20draft%20of%20guideline%20on%20cybersecurity%20and%20data%20protection.pdf?api=v2.

8 Glossary

ACC	Adaptive Cruise Control
ACSF	Automatically Commanded Steering Function
ADAS	Advanced Driver Assistance System
AEB	Autonomous Emergency Braking
(A)SIL	(Automotive) Safety Integrity Level
AUTOSAR	Automotive Open System Architecture
CEL	Complex ELectronic
CMMI	Capability and Maturity Model Integrated
CoP	Code of Practice
CSF	Corrective Steering Function
DAL	Design Assurance Level
DVSA	Driver and Vehicle Standards Agency (United Kingdom)
ECU	Electronic Control Unit
EDR	Event Detection Recorder
Euro NCAP	European New Car Assessment Programme
DSSA	Data Storage System for ACSF
FMEA	Fault Modes and Effects analysis
FMVSS	Federal Motor Vehicle Safety Standard
FTA	Fault Tree Analysis
GPSD	General Product Safety Directive
GRRF	WP.29 Working Party on Brakes and Running Gear
HAZOP	Hazard and Operability Analysis
HAV	Highly Automated Vehicle
HMI	Human Machine Interface (Interaction)
IWG	Informal Working Group
LCA	Lane Change Assist
LKA(S)	Lane Keep Assist (System)
MISRA	Motor Industry Software Reliability Association
NHTSA	National Highway and Traffic Safety Administration (United States)
ODD	Operational Design Domain
OEDR	Object and Event Detection and Response
OEM	Original Equipment Manufacturer
OICA	International Organisation of Motor Vehicle Manufacturers
OTA	Over-the-Air
RAPEX	European Community Rapid Alert System
SPICE	Software Process Improvement and Capability dEtermination
UN(ECE)	United Nations (Economic Commission for Europe)

Annex 1 PROPOSAL FOR REGULATORY TEXT AMENDMENTS TO REGULATION 79 ANNEX 6

Annex 6

SPECIAL REQUIREMENTS TO BE APPLIED TO THE SAFETY ASPECTS OF COMPLEX ELECTRONIC VEHICLE CONTROL SYSTEMS

1. GENERAL

This annex defines the special requirements for documentation, fault strategy and verification with respect to the safety aspects of Complex Electronic Vehicle Control Systems (paragraph 2.3. below) as far as this Regulation is concerned.

This annex may also be called, by special paragraphs in this Regulation, for safety related functions which are controlled by electronic system(s).

This annex does not specify the performance criteria for "The System" but covers the methodology applied to the design process and the information which must be disclosed to the technical service, for typeapproval purposes.

This information shall show that "The System" respects, under normal and fault conditions, all the appropriate performance requirements specified elsewhere in this Regulation.

Involvement of the technical service at an early stage in the design process is recommended for an effective assessment of "The System" to the requirements of this Annex.

Reason for amendment: To encourage early involvement of the TS in the development cycle to help increase understanding of safety approach for approval assessment.

2. DEFINITIONS

For the purposes of this annex,

2.1. "Safety concept" is a description of the measures designed into the system, for example within the electronic units, so as to address system integrity and thereby ensure safe operation even in the event of an electrical failure. The possibility of a fall-back to partial operation or even to a back-up system for vital vehicle functions may be a part of the safety concept.

2.2. "Electronic control system" means a combination of units, designed to co-operate in the production of the stated vehicle control function by electronic data processing. Such systems, often 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. "The System", referred to herein, is the one for which type approval is being sought.

2.3. "Complex electronic vehicle control systems" are those electronic control systems which are subject to a hierarchy of control in which a controlled function may be over-

ridden by a higher level electronic control system/function. A function which is over-ridden becomes part of the complex system.

2.4. "Higher-Level control" systems/functions are those which employ additional processing and/or sensing provisions to modify vehicle behaviour by commanding variations in the normal function(s) of the vehicle control system. This allows complex systems to automatically change their objectives with a priority which depends on the sensed circumstances.

2.5. "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.

2.6. "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.

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

2.8. "Boundary of functional operation" defines the boundaries of the external physical limits within which the system is able to maintain control.

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" 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.

3.1.1. Documentation shall be made available in two parts:

(a) The formal documentation package for the approval, containing the material listed in paragraph 3. (with the exception of that of paragraph 3.4.4.) which shall be supplied to the technical service at the time of submission of the type approval application. This will be taken as the basic reference for the verification process set out in paragraph 4. of this annex.

(b) Additional material and analysis data of paragraph 3.4.4. which shall be retained by the manufacturer, but made open for inspection at the time of type approval.

3.2. Description of the **design process methodology and** functions of "The System"

A description should be provided of the methodology applied for the design of "The System", which includes the processes and standards followed within the design and development life cycle, for example for the automotive industry these may include ISO 26262, MISRA C and Automotive SPICE. The application

of the methodology shall be demonstrated by an assessment report established by a competent authority. This may include a certificate of accreditation issued by an accreditation body.

Reason for amendment: To enforce the use of a recognised development approach, which is audited.

A description shall be provided which gives a simple explanation of all the control functions of "The System" and the methods employed to achieve the objectives, including a statement of the mechanism(s) by which control is exercised.

3.2.1. A list of all input and sensed variables shall be provided and the working range of these defined.

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 (paragraph 2.8.) shall be stated where appropriate to system performance.

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.

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

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.

3.3.4. Signal flow and priorities

There shall be a clear correspondence between these 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 as far as this Regulation is concerned.

3.3.5. Identification of units

Each unit shall be clearly and unambiguously identifiable (e.g. by marking for hardware and 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 strategy chosen to achieve "The System" objectives will not, under non-fault conditions, prejudice the safe operation of systems which are subject to the prescriptions of this Regulation.

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. The manufacturer shall be prepared, if required, to show some evidence of the means by which they determined the realisation of the system logic, during the design and development process.

3.4.3. The Manufacturer shall provide the technical authorities with an explanation of the design provisions built into "The System" so as to generate safe operation under fault conditions. Possible design provisions for failure in "The System" are for example:

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

(b) Change-over to a separate back-up system.

(c) Removal of the high level function.

In case of a failure, the driver shall be warned for example by warning signal or message display. When the system is not deactivated by the driver, e.g. by turning the ignition (run) switch to "off", or by switching off that particular function if a special switch is provided for that purpose, the warning shall be present as long as the fault condition persists.

3.4.3.1. 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 vehicle control system objective, 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, 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 on the occurrence of any one of those **identified hazards or** faults which will have a bearing on vehicle control performance or safety.

Reason for amendment: The safety approach at concept level will consider hazards, whereas at system level it will consider faults. Therefore hazards as well as faults need to be mentioned here.

~~This may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) or any similar process appropriate to system safety considerations.~~

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

The technical service shall perform an audit of the application of the analytical approach(es). The audit shall include:

- **Inspection of the safety approach at the concept (vehicle) level with confirmation that it includes consideration of interactions with other vehicle systems and reasonably foreseeable misuse by the driver[17]. This may be based on a Hazard and Operability analysis (HAZOP) or any similar process appropriate to system safety.**
- **Inspection of the safety approach at the system level. This may be based on a Failure Mode and Effect Analysis (FMEA), a Fault Tree Analysis (FTA) or any similar process appropriate to system safety.**
- **Inspection of the validation plans. This may include Hardware in the Loop (HIL) testing and vehicle on–road operational testing with expert and/or non-expert drivers or any similar testing appropriate for validation.**

Reason for amendment: To enforce audit of safety approach at both concept and system level. Concept level specifically requires consideration of interaction with other vehicle systems.

The audit shall consist of spot checks of selected hazards and faults to establish that argumentation supporting the safety concept is understandable and logical and validation plans are suitable and have been completed.

Reason for amendment: Acceptance criteria for audits above.

Recommendations may be made for tests to be performed in paragraph 4 to verify the safety concept.

Reason for amendment: Ideally, the audit should identify main safety risks for further assessment with testing.

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

[17] Note that text '**and reasonably foreseeable misuse by the driver'** was not included in proposed amendments presented at the 82nd GRRF meeting Sept 2016.

3.4.4.2 This documentation shall describe the resistance of 'The System' to environmental influences, e.g. climate, mechanical resistance and electromagnetic compatibility.

Reason for amendment: These items are specifically required by some approval authorities and therefore included to enforce established best practice.

4. VERIFICATION AND TEST

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"

As the means of establishing the normal operational levels, verification of the performance of the vehicle system under non-fault conditions shall be conducted against the manufacturer's basic benchmark specification unless this is subject to a specified performance test as part of the approval procedure of this or another Regulation.

4.1.2. Verification of the safety concept of paragraph 3.4.

The reaction of "The System" shall, at the discretion of the type approval authority, be checked under the influence of a failure in any individual unit by applying corresponding output signals to electrical units or mechanical elements in order to simulate the effects of internal faults within the unit.

It is recommended that these tests include aspects that impact on vehicle controllability and user information (HMI aspects).

Reason for amendment: Controllability and HMI are most important parts of system as regards safety and therefore should be included in tests.

4.1.2.1. The verification results shall correspond with the documented summary of the failure analysis, to a level of overall effect such that the safety concept and execution are confirmed as being adequate.

5. REPORTING BY TECHNICAL SERVICE

Reporting of the audit by technical service 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.

Reason for amendment: Traceability was found to be an important part of established best practice. This enforces it.

An example of a possible layout for the report from the technical service to the type approval authority is given in the template below (Note KBA reporting template Nr. 01-05):

Reason for amendment: Example of possible layout of report for TS to approval authority could be included to help ensure consistent interpretation of requirements. German KBA template attached, but could be made more generic if required.

Nr. 01-05

Type-Approval Procedure

Information System of the German Type-Approval Authority

0. General data

0.1 Vehicle make:

0.2 Type:

0.3 Idenfication mark: (if applicable)

0.4 Name and address of the manufacturer:

0.4.1 Name and address of the appointee:

0.5 Information folder or documentation

No.:

Date of issue:

Date of last update:

Type-Approval Procedure

Information System of the German Type-Approval Authority

1. Test vehicle(s) / object(s)

1.1 General description: *N.B.: Information to be provided either here or as an attachment*

General description of the complex electronic system with its main components and functions, as well as brief explanation of the safety concept and of the possibility of testing the operating condition of the system as part of the periodic technical inspections *(see, for instance, ECE Regulation 13, Annex 18, paragraph 3.1)*

1.2 Description of the control function: *N.B.: Information to be provided either here or as an attachment*

Specific description of all control functions and
- list of all input and measurement variables,
- list of all output variables,
- boundaries within which the system functions *(see, for instance, ECE Regulation 13, Annex 18, paragraph 3.2)*

1.3 Description of the components: *N.B.: Information to be provided either here or as an attachment*

Specification (in list form) of the discrete functional units
with their respective
- combinations of assembly in the system,
- linkages and signal flow priorities,
- information regarding the identifiability of hard- and software *(see, for instance, ECE Regulation 13, Annex 18, paragraph 3.3)*

2. Manufacturer's safety concept *N.B.: Information to be provided either here or as an attachment*

2.1 Manufacturer's declaration:

The manufacturer(s) XXX has/have confirmed that the strategy chosen for the achievement of the objectives of the "system", assuming flawless conditions, does not interfere with the safe operation of parts of the equipment required under this regulation *(e.g. braking device)* (see appendix).

Type-Approval Procedure
Information System of the German Type-Approval Authority

2.2 Hard and Software development:

Specification of the documents in which the software development process is described. Description/diagram of the software development process including the software design factors

2.3 Function in case of errors in the system:

General description of the fallback, change or shut-off functions and any possible partial operation functions, including their conditions and boundaries of their effectiveness in the event of
any failures in the "system"

Description of the simulated malfunction

2.4 Analysis of the behavior of the "system" in case of errors:

Description of the results and confirmation by the Technical Service that the corresponding documentation *(for instance in accordance with ECE Regulation 13, Annex 18, paragraph 3.4.4)* can be accessed by the approval authority through the manufacturer under its reference number XXXX.

Specification of the documents evidencing the verification of the fault-free performance of the vehicle system in operation.

2.5 Resistance against environmental influences:

E.g. type and scope of tests on climate and mechanical resistance and electromagnetic compatibility

2.6 Testability of the system:

Description of the possibility of testing the operating condition of the system as part of the periodic technical inspections

2.7 General information:

Test location:

Test date:

Type-Approval Procedure
Information System of the German Type-Approval Authority

2.8 Comments:

3. Appendices:

Appendix 1: *e.g. list of changes*

Appendix 2: *e.g. general description regarding 1.1*

Appendix 3: *e.g. manufacturer's declaration regarding 2.1*

...

4. Final certificate
Statement of conformity

The information folder referred to under item 0.5. and the type described therein – d o c o n - f o r m – to the above-mentioned test specification.

This test report consists of pages 1 to 5.

This test report may be reproduced and distributed only by the client and only in its entirety. Any partial reproduction and publication of the test report is permissible only with the prior written approval of the test laboratory.

TEST LABORATORY

accredited by the Accreditation Office of the Federal Motor Vehicle Department, Federal Republic of Germany

City Date

Order number

E-mail: firstname.lastname@td.de

Phone: XXX
Fax: YYY

Signature

Chartered Engineer

Name (please print):

HOW TO OBTAIN EU PUBLICATIONS

Free publications:

- one copy:
  via EU Bookshop (http://bookshop.europa.eu);

- more than one copy or posters/maps:
  from the European Union's representations (http://ec.europa.eu/represent_en.htm);
  from the delegations in non-EU countries
  (http://eeas.europa.eu/delegations/index_en.htm);
  by contacting the Europe Direct service (http://europa.eu/europedirect/index_en.htm)
  or calling 00 800 6 7 8 9 10 11 (freephone number from anywhere in the EU) (*).

  (*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you).

Priced publications:

- via EU Bookshop (http://bookshop.europa.eu).

Priced subscriptions:

- via one of the sales agents of the Publications Office of the European Union
  (http://publications.europa.eu/others/agents/index_en.htm).

ET-01-17-043-EN-N

Publications Office

doi: 10.2873/548794