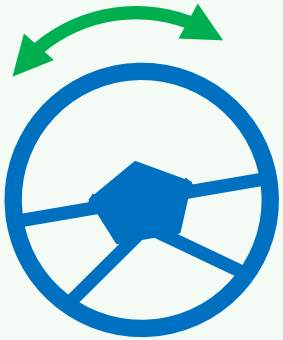
Informal Document: ACSF-16-09

Regulatory needs for ACSF
(Automatically Commanded Steering Functions)
and derivation of performance requirements

How to proceed with Category B2?

(especially B2 level 3)



Jost Gail
Oliver Bartels

Federal Highway Research Institute, Germany

Different kinds of lateral control

- B1 – SAE level 1 and 2 (hands-on) – finished

- B2 – SAE level 1 and 2 – to be finished
  - Continuous lateral control but driver has to surveil at any time (= hands-off but eyes-on?)
  - There is already a lot of effort flown into ACSF-06-28
  - Many requirements fixed because driver is per se not good in surveilling a system

- B2 – SAE level 3 – considerations to be started

Definition

B2

2.3.4.1.3.

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

up to now no discrimination between level 2 and level 3

What is needed for B2 level 3?

The step from level 2 to level 3 is per definition depending on what the driver is allowed to do:

- *lateral and longitudinal control is done by the system in level 2 as well as in level 3*
- *but monitoring the driving environment is in level 3 now the task of the system and not of the driver anymore*

-> Traffic law has to allow driving at level 3 as a prerequisite and has to define how vigilant the driver has to stay when the systems is operating

-> Technical performance of the system has to correspond to this (to the degree of the driver turning away)

What is needed for B2 level 3?

2 documents of help:

- ECE/TRANS/WP.29/2017/145 as a guidance
  (blue text)

- ACSF-06-28 as a basis
  (green text)

  (text is taken from the Category E part of the document which was discussed to the greatest extend)

  (text with regard to missing issues (to do) in red)

Essential differences of B2 level 3 compared to level 2

- “hands-off and eyes off”
- “driver out of the loop” as long as the system is in its ODD (=Operational Design Domain)

  (The driver may perform secondary activities; he is not obliged to surveil the system, he only has to stay prepared for a transition demand; that means e.g. not to leave the seat or not to sleep)

->All object and Event Detection and Response (= OEDR) has to be done by the system

Consequences of the fact that the driver is not obliged in level 3 to monitor the driving environment and to respond immediately

(1) System has to handle the driving task during the specified use case or ODD alone

-> System must cope with a bundle of difficult traffic situations with result from the specific ODD

- New specific performance requirements for various conditions
- More specification tests
- More cases to be demonstrated by the OEM
- More proof by simulation?

Consequences of the fact that the driver is not obliged in level 3 to monitor the driving environment and to respond immediately

(2) Significantly more lead time for transition than for B2 level 2 (there we rather fixed a “hands-on-time”)

(3) B2 level 3 has to be fail-operational, at least as long as the transition procedure is taking place

-> Requirements for functional safety and redundancies have to be set (ISO 26262, ASIL D?)

(4) System performance has to correspond to the activities that are allowed for the driver during the ODD

How to organise thinkable use cases or ODDs for level 3 B2 systems?

- by roadway (motorway, inter-urban, urban)?

  -> first highway

  -> first between exits?
- by speed?

  -> up to 130 km/h
- by traffic situation (e.g. congestion)?

  -> not considered yet

Step-by step:

What is needed for B2 level 3 and what did we already fix?

Basic characteristics of a level 3 system

- The system is able to cope with all dynamic driving tasks within its Operational Design Domain (ODD) or will otherwise transit to the driver offering sufficient lead time (driver is fallback).
- The system drives and monitors (specific to the ODD) the environment.
- The system detects system limits and issues a transition demand if these are reached.

Vehicle tasks – vehicle movements and monitoring of the environment

- Execute longitudinal (accelerating/braking) and lateral (steering) portions of the dynamic driving task when activated. Shall monitor the driving environment for operational decisions when activated.

-> It has to be considered

- which regulatory provisions for longitudinal (accelerating, braking) and lateral control (steering) are necessary
- which quality of and area of monitoring of the driving environment is necessary

Vehicle tasks – vehicle movements

5.6.1.1.4 The specified maximum speed v_{smax} shall not have a value of more than 130 km/h

5.6.1.1.5. The specified maximum lateral acceleration ay_{smax} shall not have a value of more than 3 m/s² and, if v_{smax} is > 60 km/h of less than 1 m/s².

5.6.1.1.6. The activated system shall at any time control the movement of the vehicle in such a way that the vehicle does not induce any safety critical situations and that the movements of the vehicle are clear to other road users.

5.6.1.2.4. The activated system shall ~~prior and after a lane change manoeuvre~~ ensure that the vehicle does not cross any lane marking.

5.6.1.7.1. Any vehicle equipped with an ACSF of category E shall be able to control the longitudinal speed of the vehicle

5.6.1.7.1.1. If the activated system detects that the distance to other road users in front is less or will shortly be less than the foreseen safety distance a protective deceleration shall be carried out until the foreseen safety distance is reached again.

Missing since long. and lat. control is both done without driver control:

- **A system B2 of level 3 has to follow each curve by adapting speed**
- **Define appropriate tolerances for speed and lateral acc. to avoid problems we experienced with Cat. B1**

Vehicle tasks – monitoring of the environment

5.6.1.1.8. The vehicle shall be equipped with means to monitor at any time when ACSF is active a minimum range to the front (s_{Front}), to the right (s_{side}), and to the left side (s_{side}) and behind (s_{Rear}) the vehicle with the purpose to avoid or to mitigate collisions.

5.6.1.1.8.1. The minimal range in front (s_{Front}) of the ACSF vehicle shall be calculated according to the following formula:

$$s_{Front} = v_{ACSF}^2 / (2 \cdot a_{ACSF})$$

where:

s_{Front} = *relative distance between the vehicle equipped with ACSF and the vehicle driving in front, measured in meters from the front edge of the vehicle equipped with ACSF to the rear end of the vehicle driving in front.*

v_{ACSF} = *speed of the vehicle equipped with ACSF measured in m/s*

a_{ACSF} = *3,7 m/s² = feasible deceleration under wet conditions*

5.6.1.1.8.3. The minimal range to the left and to the right (side) shall be at least 7 m (measured from the medium longitudinal centerline of the vehicle *equipped with ACSF*)

Vehicle tasks – activation / deactivation / override

- Permit activation only under conditions for which it was designed. System is deactivated immediately at the request of the driver. However the system may momentarily delay deactivation when immediate human takeover could compromise safety.

-> It has to be considered

- to ensure that the system permits activation only under conditions for which it was designed
- to ensure that the system deactivates immediately upon request by the driver (or delays deactivation when immediate driver takeover could compromise safety)
- to ensure that overriding by the driver is possible at any time

Vehicle tasks – activation / deactivation / override

5.6.1.2. Operation of ACSF

5.6.1.2.1. Any system operation ~~lane change manoeuvre~~ shall take place ~~be initiated~~ only if:

5.6.1.2.1.

- the vehicle is travelling on a road section which is not dedicated to pedestrians or cyclists and which has a [physical or constructional] separation of traffic moving in opposite directions and which has at least two lanes for the direction the vehicle is driving and
- any traffic that can affect the safe ~~manoeuvre~~ operation is identified by equipment installed on the vehicle and
- the vehicle equipment can analyze speed and distance of the identified traffic to ensure a safe ~~manoeuvre~~ operation (e.g. does not cause a deviation to the flow, direction of other traffic or considering left- or right-hand traffic).

Vehicle tasks – activation / deactivation / override

2.4.8.13. "ACSF status" means any distinct operational mode of the ACSF like "switched off" "switched on", "available to be activated", "activated" etc.

2.4.8.19. An ACSF is in “off mode” (or “switched off”) when prevented from controlling the steering system.

2.4.8.20. An ACSF is in “standby mode” when the function is switched on but the conditions for being active are not all met. In this mode, the system does not control the steering system.

2.4.8.21. An ACSF is in “active mode” (or “active”) when the function is switched on and the conditions for being active are met. In this mode, the system [continuously or discontinuously] controls the steering system.

2.4.8.22. An ACSF is in “failure mode” when the system has detected a failure.

5.1.6.1. Whenever an Automatically Commanded Steering function becomes active, this shall be indicated to the driver. Any termination of control shall produce a warning in accordance with the requirements of paragraph 5.4.3.

5.4.3. Special Warning Provisions for Automatically Commanded Steering Functions

Vehicle tasks – activation / deactivation / override

5.4.3.1 Any termination of control initiated by the system (i.e. when the active mode is automatically deactivated by the system), other than specified in 5.6.1.4.7 shall produce a distinctive driver warning including visual warning and either an acoustic warning or an haptic warning until the driver has resumed steering control or the vehicle is at standstill. The same warning as for a transition demand maybe used. In the case of ACSF category A, a short [but distinctive] warning is deemed to fulfill the warning requirement above. In the case of ACSF category B1, no warning is necessary.

5.6.1.1.1. [The system shall be active (deliver automatic steering) only after a deliberate action of the driver and if the conditions for operation of the system are fulfilled (all associated functions – e.g. brakes, accelerator, steering, camera / radar / lidar etc. are working properly).]

5.6.1.1.2. The vehicle shall be equipped with a means for the driver to activate and deactivate the system. The deactivation shall be possible at any time.
The activation of the system shall not be possible if the driver is not in the driver seat or if the seatbelt is not fastened.

5.6.1.1.7. The system status shall be indicated to the driver by a visual signal. The indication shall [at least] distinguish between stand-by, active and failure Mode. The indication shall be present as long as the relevant system status persists.

Vehicle tasks – activation / deactivation / override

5.6.1.1.3. [Deliberate braking operation by the driver shall take priority over a demand for longitudinal movement by the ACSF system.
Deliberate Accelerating operation by the driver shall take priority over a demand for longitudinal movement by the ACSF system.
Deliberate Steering operation by the driver shall take priority over a demand for steering by the ACSF system.
The system may remain active provided that priority is given to the driver during the overriding period. The means to override the ACSF shall be indicated in the system information data. A transition demand may be issued at the discretion of the vehicle manufacturer to request the driver for [an orderly] takeover.]

Vehicle tasks – Coping with traffic situations and when to issue a transition demand

- The system is able to cope with all dynamic driving tasks within its Operational Design Domain (ODD) or will otherwise transit to the driver offering sufficient lead time (driver is fallback).
- The system detects system limits and issues a transition demand if these are reached.

-> It has to be considered

- which traffic situations the system has to master
- which kind of situations have to result in a transition demand (depending on the boundaries of the ODD)
- which value of lead time is sufficient

Vehicle tasks – Transition (lead time and MRM)

- System is automatically deactivated only after requesting the driver to take-over with a sufficient lead time; may – under certain, limited circumstances – transit (at least initiate) to minimal risk condition if the human driver does not take over. It would be beneficial if the vehicle displays used for the secondary activities were also used to improve the human takeover process.

-> It has to be considered

- to ensure the system automatically deactivates only after requesting the driver to take-over with a sufficient lead time
- to care for an appropriate minimal risk condition
- how to reengage the driver following system request (multiple sensory channels / one might use vehicle displays for the secondary activities to improve the human takeover process)

Vehicle tasks – Coping with traffic situations and when to issue a transition demand

2.4.8.8. "Normal operating conditions" mean that the ACSF system is active and does neither carry out a transition procedure nor a Minimal Risk Manoeuvre nor an Emergency Manoeuvre.

2.4.8.9. "Transition demand " means an instruction from the ACSF that the driver has to take over control of the steering task again.

2.4.8.10. "Transition procedure" means the sequence of providing a transition demand by the system, taking over steering control by the driver and deactivation of the ACSF.

2.4.8.11. "Conditions for operation" mean circumstances like traffic situation, road category, quality of lane markings, vehicle speed, curvature of the road, lighting, sensor capabilities etc. specified by the vehicle manufacturer, where the system is designed to operate.

(= ODD)

2.4.8.12. "System boundaries" mean all circumstances from which on the conditions for operation are not fulfilled anymore.

Vehicle tasks – Coping with traffic situations and when to issue a transition demand

5.6.1.2.5. The system shall detect if the driver's seatbelt is unfastened. When the driver's seatbelt is detected to be unfastened a transition demand shall be initiated according to 5.6.1.4.4.

5.6.1.4. Transition demand and system operation during transition

5.6.1.4.1. If the system detects that its boundaries are reached or will be reached shortly or in case of a system failure it shall provide a transition demand.

5.6.1.4.2. The timing of the transition demand shall be such that sufficient time is provided for a safe transition to manual steering.

5.6.1.4.2.1. In case of normal operating conditions and in case that the system anticipates that system boundaries will be reached a transition demand shall be given not later than 4 s before system boundaries are reached.

5.6.1.4.2.2. In case of a sudden unexpected event with imminent danger of a collision a transition demand shall be given immediately and an emergency manoeuvre shall be initiated.

Vehicle tasks – Coping with traffic situations and when to issue a transition demand

5.6.1.4.2.3. In case of a sudden unexpected event without imminent danger of a collision a transition demand shall be given immediately and the system shall follow the [system / basic]* desired path for at least 4 s after the transition demand, at least in the following cases

- if the speed of the vehicle with activated ACSF exceeds v_{smax}, or
- if the vehicle with activated ACSF and a specified v_{smax} > 60 km / h, reaches a lateral acceleration of more than ay_{smax} , or
- if a system boundary is reached due to a missing lane marking, or - if a single sensor failure occurs.

5.6.1.4.3. If a transition demand is given because a driver availability recognition system according 5.6.1.6, the system shall follow the [system / basic]* desired path for at least 4 s after the transition demand has started.

5.6.1.4.~~4~~. The system shall provide a transition demand if the driver's seatbelt is unfastened or if the driver's seat is left by the driver. In this case the system shall follow the initial path at least [4 s] after the transition demand.

Vehicle tasks – Coping with traffic situations and when to issue a transition demand

5.6.1.4.5. In case of other failures than a single sensor failure a transition demand shall be given immediately and the system shall initiate the fail-safe strategy as declared by the manufacturer in Annex 6 of this regulation, as soon as the failure is detected.

5.6.1.4.6. In case the vehicle is fitted with a built-in infotainment system, content visible to the driver, which is not relevant for driving, shall be deactivated as long as a transition demand is issued.

5.6.1.4.7. The transition demand shall be provided by a visual warning signal and either an acoustic warning signal or by imposing a haptic warning signal. The warning shall be escalating with time in terms of enlarging the intensity of the warning and/or in terms of adding and/or changing the warning means, or start immediately with the highest intensity level.

For level 3 the discrimination into “system anticipates boundary” and “sudden unexpected event with or without imminent danger of collision” is not necessary anymore because the system always has to deliver sufficient lead time; in addition the 4 s lead time is too less and has to be changed!

Vehicle tasks – Coping with traffic situations and when to issue a transition demand

Need to define typically occurring difficult traffic situations that have to be mastered or that have to result in a transition demand because the boundaries of the ODD will be reached:

Construction area

Narrow lane

Narrow curve

Inclement weather

Other vehicle cutting in

Other vehicle cutting out with obstacle in front

Different kind and sizes of obstacles

Deer

Other vehicle broken down and covering lane only partly (plus pedestian aside this car?)

Low mu

Different kinds of failures

Vehicle tasks – Transition (MRM)

2.4.8.15. "Minimal risk manoeuvre" means a procedure aimed at minimizing risks in traffic, which is automatically performed by the system, e.g. when the driver does not respond to a transition demand

6.1.5. Minimal Risk Manoeuvre 5.6.1.5.1. If the system detects that after a transition demand the driver does not take over manual control of the steering again the vehicle shall carry out a minimal risk manoeuvre not later than 4 s after the start of the transition demand

5.6.1.5.2. It shall at any time be possible to override the minimal risk manoeuvre by the driver. The system may be designed to exclude unintended override.

5.6.1.5.3. The hazard lights shall be activated automatically not later than 10 s after the start of the minimal risk manoeuvre. Additionally, an audible warning device may be permitted to warn the other road users.

For level 3 the course of the MRM shall be defined: Decelerate the vehicle carefully and bring it to a safe stop

Vehicle tasks – driver availability recognition

- Driver availability recognition shall be used to ensure the driver is in the position to take over when requested by the system. Potential technical solutions range from detecting the driver's manual operations to monitoring cameras to detect the driver's head position and eyelid movement.

-> It has to be considered

- that an appropriate means for driver availability recognition is used to ensure the driver is in the position to take over the driving task when requested by the system or when required

  -> Detection of e.g.

  – seated/unseated,
  – head and/or eye movement and/or input to any control element of the vehicle

Vehicle tasks – driver availability recognition

2.4.8.14. “Driver availability recognition [system / function]” means a function able to assess driver’s physical availability to respond to a transition demand from an ACSF system.

5.6.1.2.6. Driver availability recognition system

The system shall comprise a driver availability recognition system that is active whenever the ACSF system is active.

The driver availability recognition system shall detect that the driver is present in the driver seat and that he is available to take over the steering.

5.6.1.2.6.1. Driver not present in the driver seat

When the driver is not present in the driver seat the system shall provide a distinctive warning until the driver is detected to be back in the driver seat or until a transition demand is initiated.

When the driver is not back in the driver seat during the distinctive acoustic warning with a max. duration of [15 s] a transition demand shall be initiated according to 5.6.1.4.3.

Vehicle tasks – driver availability recognition

5.6.1.2.6.2. Driver not available to take over the steering

The system shall check if the driver is available to take over the steering by permanently evaluating driver's activity. The means to detect driver's activity [(e.g. head and/or eye movement and/or input to any control element of the vehicle)] shall be selected by the manufacturer. When the driver does not show any activity for a time span of maximum [3] min the system shall provide a distinctive acoustic warning until appropriate actions of the driver are detected (e.g. the driver resumes manual control) or until a transition demand is initiated.

When the system does not detect appropriate actions from the driver during the distinctive accoustic warning with a max. duration of [15 s] a transition demand shall be initiated according to 5.6.1.4.3.

Is the text appropriate for B2 level 3 where the driver is allowed to turn away (and perhaps is not obliged to show activity)?

Vehicle tasks – emergency manoeuvres

- Emergency braking measures must be accomplished by the system and not expected from the driver (due to secondary activities).

-> It has to be considered

- that there are provisions for emergency braking (or even emergency steering) measures by the system if the time for a proper transition procedure is too short

Vehicle tasks – emergency manoeuvre

2.4.8.16. "Emergency Manoeuvre" is a manoeuvre performed by the system in case of a sudden unexpected event in which the vehicle is in imminent danger to collide with another object, with the purpose to avoid or mitigate a collision.

2.4.8.17. "Protective braking" means an application of the brakes of the vehicle by the system in order to decelerate the vehicle with the purpose of avoiding or mitigating a collision.

5.6.1.6. Emergency Manoeuvre

5.6.1.6.1. If the activated ACSF detects that due to a sudden unexpected event the vehicle is in imminent danger of a collision and that the time for a safe transition procedure is too short, an emergency manoeuvre shall be carried out (e.g. by braking the vehicle and/or by steering).

5.6.1.7.1.2. If the activated system detects that due to a sudden unexpected event the vehicle is in imminent danger to collide with another road user in front and that the time for a safe transition procedure is too short, a protective deceleration as emergency manoeuvre shall be carried out. Only in case a lane change can be carried out safely, alternatively a lane change manoeuvre can be carried out to prevent the collision.

5.6.1.7.1.3. The protective deceleration must be able to deliver full braking force of the vehicle in order to achieve a maximum deceleration.

Since driver is allowed to turn away in level 3, emergency manoeuvres must intervene in a bundle of thinkable situations (need to collect and list these)

Vehicle tasks – system reliability

- Consideration shall be given to evaluation of the system reliability and redundancy as necessary.

-> It has to be considered

- which requirements for functional safety and redundancies have to be set (ISO 26262, ASIL level, fail-operational) for steering and braking (sensors, actuators, energy supply,...)

- **Up to now there is only Annex 6**

Vehicle tasks – data storage

- Recording of system status (inc. system behavior)
  (DSSA-Data Storage System for ACSF, EDR, etc.)

-> It has to be considered

- which kind of recording is necessary and which content shall be recorded (driver's operations / system status / system behaviour)

Vehicle tasks – data storage

[2.4.8.18. " Data Storage System for ACSF (DSSA)“ means a data recording medium to record ACSF system operation data including data of Driver availability Recognition System.]

[5.6.1.8.1. The DSSA shall record and store the data during the operation of the ACSF in order to demonstrate ~~that~~ if the ACSF had operated properly in align with the relevant requirements in case of a road accident The DSSA shall be fitted in the vehicle and should not contain any radio interface. The DSA shall be designed to ensure data security and data protection and shall be protected against tampering and misuse. The driver and the passengers of the vehicle have to be adequately informed about the data capture. Principally, they shall be enabled to decide by themselves by several options about the processing of the data.

5.6.1.8.2. The DSSA shall record and store following data:

GPS-time

GPS Location

Information about the ACSF status

Information about failures

Information about transition demands

Information about minimal risk manoeuvre

Takeover of the steering by the driver

Vehicle tasks – data storage

5.6.1.8.3. The recorded data shall not be deletable and not be volatilized in the DSSA without any deterioration [for at least [6] month].

5.6.1.8.4. If special tools are necessary to get access to recorded data, the tools shall be made available by the manufacturer to the authorities, the driver and the passengers of the vehicle and the vehicle owner.

5.6.1.8.5. The DSSA shall record at least for [30] seconds prior to and [10] seconds after an accident.]

Vehicle tasks – PTI

- Offering the possibility to carry out a beneficial periodical check of roadworthiness

-> It has to be considered

- how to verification of correct operational status in a simple way
- to use a failure warning signal
- to use an electronic communication interface
- how to do the confirmation of valid software version

Vehicle tasks – PTI

5.5.2. It shall be possible to verify in a simple way the correct operational status of those Complex Electronic Systems, which have control over steering. If special information is needed, this shall be made freely available. [It shall be possible to verify the correct operational status of those Electronic Systems by a visible observation of the failure warning signal status, following a "power-ON" and any bulb check.

In the case of the failure warning signal being in a common space, the common space must be observed to be functional prior to the failure warning signal status check.

In the case of an ACSF system able to operate at higher speed than 10km/h, it shall be possible to confirm the failure warning signal status via the use of an electronic communication interface.]

In the case of an ACSF system it shall be possible to confirm the valid software version of the system via the use of an electronic communication interface.

5.5.2.1. At the time of Type Approval the means implemented to protect against simple unauthorized modification to the operation of the verification means chosen by the manufacturer (e.g. warning signal) shall be confidentially outlined.

Alternatively this protection requirement is fulfilled when a secondary means of checking the correct operational status is available, e.g. by using an electronic communication interface.

Vehicle tasks – traffic law

- Compatibility with traffic law

-> It has to be considered

- to ensure that the system operates in accordance with the traffic law of the country the vehicle is driving in

  [WP.1-IWG-AD recommends WP.1 to state that the use of these functions remain within the requirements of the Conventions.]

Vehicle tasks – traffic law

[5.6.1.1.x The vehicle shall detect the max. speed limit of the country, where it is used and shall not activate the ACSF system above this speed limit.]

Needed:

Detection of actual speed limit

(traffic signs, subsigns)

Detection of signs of policemen

Detection of sirens, blue and yellow light

Detection of contact with other object

Driver tasks

There are still some in level 3, namely …

- 1. Determine when activation or deactivation of the automated driving system is appropriate?
- 2. Does not need to execute the longitudinal, lateral driving tasks and monitoring of the environment for operational decisions in the ODD.
- 3. Shall remain sufficiently vigilant as to acknowledge the transition demand and, acknowledge vehicle warnings, mechanical failure or emergency vehicles.
- 4. May turn his attention away from the complete dynamic driving task in the ODD but can only perform secondary activities with appropriate reaction times. It would be beneficial if the vehicle displays were used for the secondary activities.

Driver tasks influence needed system performance level

Thus the system and the information given to the driver has to be designed in a way that the driver always knows

- which part of the driving task is carried out by the system
- which kind of behaviour is expected from him
- which tasks are expected to be carried out by him
- which activities are allowed and which are forbidden

5.6. Information about the transition procedure and the consequences of delayed or omitted take over of the steering shall be provided to the users of the vehicle, at least in the owners manual.

Needed: Better description of the information that must be given (where and when)

Other jobs

Check of all definitions if complete and appropriate

Description of tests


Thank you!