Adaptive Exterior Light and Speed Control System

Frank Houdek and Alexander Raschke

Version history

Version	Date	Comment
1.0	July 16, 2019	Initial version
1.1	July 23, 2019	Revision and extension of traffic sign detection
1.2	Aug. 1, 2019	Minor layout changes and spelling improved
1.3	Sept. 19, 2019	Correction of requirements ELS-8, ELS-12, ELS-14, ELS-15, ELS-16, ELS-17, ELS-18, ELS-19, ELS-28, ELS-32, ELS-34, Deletion of ELS-20. Splitting signal `pitmanArm` into `pitmanArmForthBack` and `pitmanArmUpDown` *Source:* Discussion with and feedback from Amel Mammar (August 25 to September 19)
1.4	Sept. 27, 2019	Clarification of ELS-47 *Source:* Case study Q&A session, (September 27)
1.5	Oct. 15, 2019	Rephrasing of all statements using the term "released" due to its ambiguity *Source:* Discussion with Amel Mammar (October 13)
1.6	Oct. 15, 2019	Clarification of ELS-21. *Source:* Discussion with Amel Mammar (October 14)
1.7	Oct. 15, 2019	Clarification of ELS-31. *Source:* Discussion with Amel Mammar (October 11)
1.8	Oct. 21, 2019	Adding priority between ELS-16 and ELS-17. *Source:* Question by Amel Mammar (September 9)
1.9	Oct. 23, 2019	Clarification of ELS-24, modification of ELS-27 (both cornering lights are activated while driving backwards).
1.10	Nov. 11, 2019	Addition of 220m in ELS-48. Clarification of Examples in SCS-5, SCS-7, SCS-8, SCS-9. Adding priority between ELS-15- and ELS-17. *Source:* Questions by Amel Mammar (November 10)
1.11	Nov. 18, 2019	Modification of ELS-40 (now all three brake lights flash in emergency braking). Mentioning tail lamps in ELS-29. Mentioning `pitmanArmForthBack` and `pitmanArmUpDown` instead of `pitmanArm` in Section 4.1 (see Version 1.3). *Source:* Questions by Nuno Macedo (November 15)
1.12	Nov. 22, 2019	Removal of word "adaptive" in description of signal `setVehicleSpeed`. *Source:* Questions by Michael Leuschel (November 22)

Version history (con't)

Version	Date	Comment
1.13	Nov. 25, 2019	Adding valid range for desired speed and its implication on cruise control lever behavior (SCS-1 to SCS-12). *Source:* Questions by Michael Leuschel (November 22)
1.14	Nov. 28, 2019	Clarification of ELS-49. *Source:* Suggestion by Amel Mammar (November 28)
1.15	Dec. 3, 2019	Correction of the examples in SCS-7, SCS-8, and SCS-9. Modification of signal description `setVehicleSpeed` *Source:* Suggestion by Amel Mammar (December 2)
1.16	Dec. 17, 2019	SCS-9, SCS-7: replacing 'target speed' by 'desired speed'. Partial reformatting of Section 5.1. Clarification of controlling vehicle speed in Section 5.3. SCS-15: Hint added that this requirement is handled by the engine directly (see Section 5.3). Adjustment of the maximum acceleration and deceleration values in SCS-20, SCS-22. SCS-23: modified to 'is 20km/h or below'. SCS-28: Clarification of priority between adaptive cruise control and emergency braking assistant in case of brake activation. *Source:* Questions by Amel Mammar (December 16)
1.17	Dec. 19, 2019	Extended explanation in Section 5.3. Modification of Traffic Sign Detection. *Source:* Observation while creating validation scenarios

Adaptive Exterior Light and Speed Control System

Frank Houdek[1] and Alexander Raschke[2]

[1] Daimler AG, Research and Development, Stuttgart, Germany
frank.houdek@daimler.com
[2] Inst. of Software Engineering, Ulm University, Germany
alexander.raschke@uni-ulm.de

1 Introduction

This case study continues the successful series of case studies for formal specification and verification of the ABZ conference series, which started with the landing gear system[1] and expanded with the hemodialysis medical device[4] and the European Train Control System (ETCS)[2] in the following years. This document describes two systems from the automotive domain: an adaptive exterior light system (ELS) and a speed control system (SCS). This specification is based on the SPES XT running example[3]. Besides their general architectures, the requirements of the software based controllers are described. Both systems are only loosely coupled, which makes it possible to handle them independently.

Conventions. Throughout this document, we use the following conventions to better distinguish different terms: **Main functions** are set in bold, *sub-functions* are italicized. Predefined `signals` are written in typewriter and for the values of signals we use a font without serifs.

The structure of the document is as follows: First, the general hardware architecture of a modern car is sketched in Sect. 3. Then, the adaptive exterior light system is described in Sect. 4, followed by the requirements of the speed control system (Sect. 5). For each of the systems, the user interface, the needed sensors and the available actuators are described before the different features are explained in detail. In Sect. A, all available signals and their value ranges are summarized in a table.

2 Disclaimer

The example in this document is inspired from real-world systems as they are available in many recent cars. However it is important to note that the given description does not describe a current or past real-world system of any vehicle of the Daimler AG.

3 General Architecture

A modern car offers many different safety and comfort functions. Most of them are nowadays realized in software running on a bunch of electronic control units

(ECUs) with connected actuators and sensors. These ECUs are connected via several bus and network techniques like CAN, LIN, or FlexRay (depending on the needed band width and reliability). The avoidance of a single central unit is three-fold: First, the risks with a single-point of failure are reduced, second, the limited space and energy of a car restricts the possible technologies, and third, there is the constant need to balance the weight and space consumption of wiring harness with space and weight consumption of decentral control units that are placed nearby the actuators. Despite the pressure to realize more and more in software, some functions are still implemented in hardware. For example, in this specification it is assumed that the detection of a defective bulb is realized by a corresponding electronic circuit.

Additional to the complexity of a distributed system, each car can be configured individually, either by law restrictions of different countries or by customer's preferences. For example, the rear direction indicator in USA and Canada is realized by a blinking red tail light, whereas in Europe it is an extra yellow light.

Figure 1 presents an exemplary excerpt of a connection diagram for the two systems described in this case study. In this case study, we do not focus on the communication between the different ECUs which is necessary because of the distribution of each functionality over several ECUs. For example, to realize left blinking, the body controller front, the door control unit left, and the body controller rear must be involved to execute the commands given by the steering column switch module. In this case study, we focus on the functionalities and simplify reality by allowing signals to be read and commands to be sent directly.

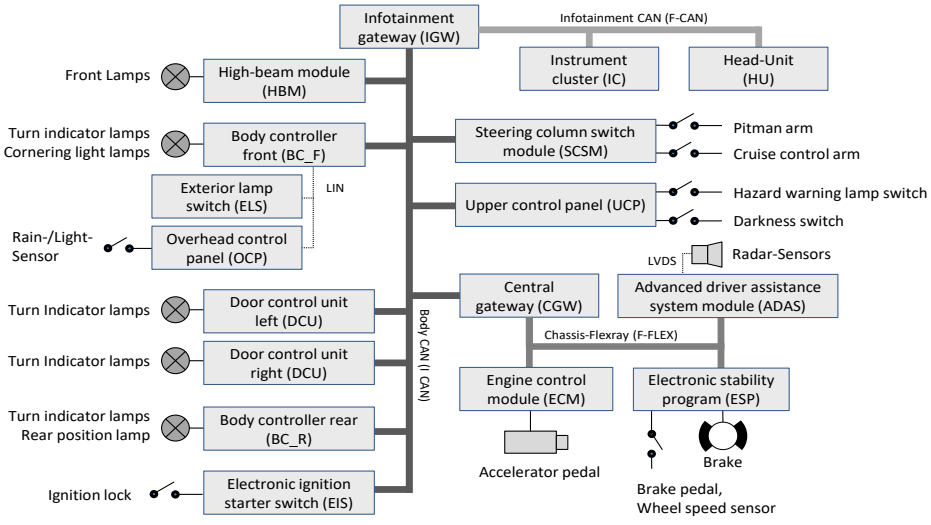

Fig. 1: System Overview

In order to save costs, the software of each control unit is parameterized with the different necessary configurations according to the country specification and the individual order. In the context of this case study, the following parameters are defined. They must be taken into account for the formal specification.

- `driverPosition` holds the information, if the car is configured for left-hand or right-hand traffic.
- The Boolean `armoredVehicle` indicates, if the current car is an armored vehicle or not.
- The `marketCode` parameter specifies the market for which the car is to be built. Some example codes are: 001 = USA, 002 = Canada, 003 = EU.

4 Adaptive Exterior Light System

The headlights of a modern car are no longer simply switched on and off by a simple mechanical switch, but the exterior light system integrates various subsystems, like the control of turn signals and comfort functions such as a cornering light. Specifically the following light system functions, among others, are described in detail in this study:

- **Turn Signal**: Control of the driving direction indicators.
- **Low beam headlights**: Control of the low beam headlights. If *daytime running light* is activated, low beam headlights are active all the time and *ambient light* illuminates the vehicle surrounding while leaving the car during darkness. The function low beam headlight also includes *parking light*.
- **Cornering light**: Control of additional headlights that illuminate the cornering area separately when turning left or right.
- **Adaptive high beam**: Control of the high beam headlights.
- **Emergency brake light**: Following drivers are warned by a flashing brake light in case of an emergency brake.

In the following sections, we first introduce the user interface, necessary sensors and the attached actuators of an exterior light system.

4.1 User Interface

The car driver can control the different functions of the lighting system by several buttons and switches, which are described in the following.
The light rotary switch has the following positions: Off, Auto, On (see Fig. 2). The light rotary switch position is transmitted via the signal `lightRotarySwitch`.

The control lever attached to the steering column is called pitman arm and allows for the following movements (see Fig. 3). The pitman arm position is transmitted via the signals `pitmanArmForthBack` and `pitmanArmUpDown`.

- By pushing away from the driver ④ (backward): Permanent activation of the adaptive high beam (with pitman arm engaged).

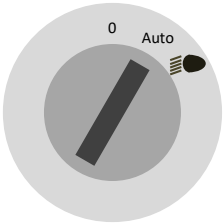

Fig. 2: Light rotary switch

- By pulling towards the driver ① (forward): Temporary activation of the high beam (without engaging, so-called flasher).
- By moving up or down ②/③: Temporary or permanent activation of the direction indicator to the left or right. The temporary activation (so called tip-blinking) happens by a deflection of about 5° (Downward5, Upward5), the permanent activation (engage) by about 7° deflection (Downward7, Upward7). The engagement ends either by manually bringing the pitman back to neutral position or automatically by a mechanical reset mechanism if the steering wheel has been turned more than 10°.
- The neutral position of the pitman arm is signaled by Neutral.

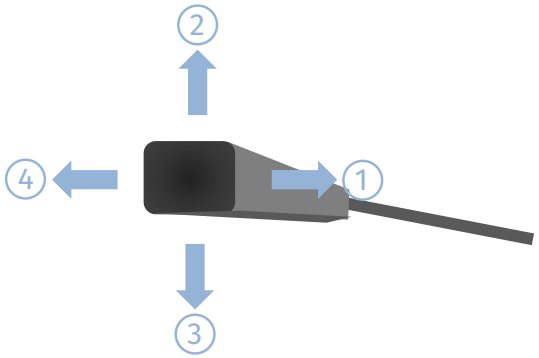

Fig. 3: Pitman arm with four directions of movement

The Hazard Warning Light Switch (see Fig. 4, `hazardWarningSwitchOn`) is just like the Darkness Switch (only available at armored vehicles, see Fig. 5, `darknessModeSwitchOn`) a simple toggle switch which turns on the corresponding function when pushed (value True) and turns it off when pushed again (value False).

The user can activate or deactivate the functions *daytime running light* and *ambient light* in the instrument cluster settings menu (which is not de-

Fig. 4: Hazard Warning Light Switch

Fig. 5: Darkness Switch (only armored vehicles)

scribed in this specification). The instrument cluster settings are transmitted via `daytimeLights` and `ambientLighting`.

4.2 Sensors

Besides the elements that can be manipulated by the user, several sensors are necessary to provide the desired features.

- Status and position of the key (and thus the information, if the ignition is on). This information is transmitted via `keyState` and has the values NoKeyInserted, KeyInserted, KeyInIgnitionOnPosition.
- Engine status `engineOn` (True, False).
- Brightness of the environment `brightnessSensor`, offering the measured outside brightness in values 0 to 100000.
- Deflection of the brake pedal `brakePedal`, where 0 means no deflection and 225 means a maximum deflection of 45°.
- Available battery voltage `voltageBattery`, measured in 0.1V.
- Angle of the steering wheel `steeringAngle`.
- Information about the status of the doors (open or closed). For the sake of simplicity there is only the information available if all doors are closed or not (via `allDoorsClosed`).
- A camera to detect oncoming vehicles, signaled via `oncommingTraffic`. The state of the camera (Ready, Dirty, NotReady) is signaled via `cameraState`.
- The current vehicle speed is available via `currentSpeed`.
- If the reverse gear is engaged, `reverseGear` becomes True.

4.3 Actuators

Figure 6 schematically shows the possible positions A (front), B (exterior mirror), C (rear), and D (rear center) of exterior lighting elements of a vehicle.
The following lighting actuators[3] are installed at the given positions (each left and right, except D which exists only once):

- Direction indicator (blinker) (A, B, C), controlled via the signals `blinkLeft` and `blinkRight`.

[3] Details about the design of the lighting elements are regulated by the directive 93/92/EEC.

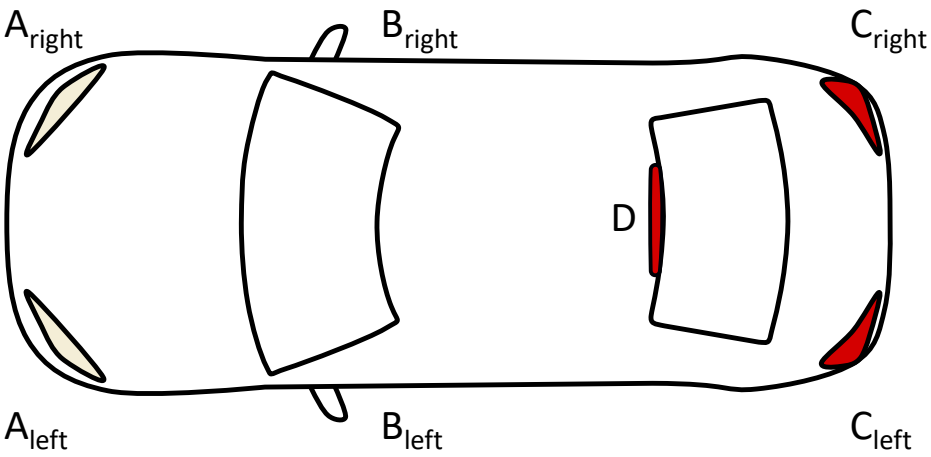

Fig. 6: Schematic position of the exterior lighting elements

- Headlights for low beam headlight (A), controlled via `lowBeamLeft` and `lowBeamRight`.
- Headlights for high beam headlight (A), controlled via `highBeamOn` to activate and deactivate the high beam, `highBeamRange` to control the high beam luminous, and `highBeamMotor` to control the high beam illumination distance.
- Lamp for cornering light left or right (integrated in front bumper) (A), controlled via `corneringLightLeft` and `corneringLightRight`.
- Brake lamp (C,D), controlled via `brakeLight`
- Tail lamp (C), controlled via `tailLampLeft` and `tailLampRight`.
- Reverse lamp (C), controlled via `reverseLight`.

Cars that are sold in USA or Canada do not have a separate direction indicator at position C. Here, the tail lamps take on the task of the rear indicator lamps.

4.4 Functional Requirements

This section lists the functional requirements for the different functions of the adaptive light system. These functions are not completely independent of each other. Moreover, they interfere at several points, mainly because of the shared use of the given actuators.

Direction blinking. The function direction blinking defines different ways to indicate the desired direction of the driver at crossings or at lane changes. It is only available, if the ignition is on (KeyInIgnitionOnPosition).

ELS-1 *Direction blinking left*: When moving the pitman arm in position "turn left" ③, the vehicle flashes all left direction indicators (front left, exterior mirror left, rear left) synchronously with pulse ratio bright to dark 1:1 and a frequency of 1.0 Hz ± 0.1 Hz (i.e. 60 flashes per minute ± 6 flashes).

ELS-2 *Tip-blinking left*: If the driver moves the pitman arm for less than 0.5 seconds in position "Tip-blinking left", all left direction indicators (see Req. ELS-1) should flash for three flashing cycles.

ELS-3 If the driver activates the pitman arm in another direction or activates the hazard warning light switch during the three flashing cycles of the tip-blinking, the tip-blinking cycle must be stopped and the requested flashing cycle must be started (i.e. direction blinking, tip-blinking, or hazard warning light, depending on the interrupting request)

ELS-4 If the driver holds the pitman arm for more than 0.5 seconds in position "tip-blinking left", flashing cycles are initiated for all direction indicators on the left (see Req. ELS-1) until the pitman arm leaves the position "tip-blinking left".

ELS-5 *Direction blinking right* and *tip-blinking right*: Analogous to the left side (see Req. Req. ELS-1 to Req. ELS-4).

ELS-6 For cars sold in USA and Canada, the daytime running light must be dimmed by 50% during direction blinking on the blinking side.

ELS-7 If the driver activates the pitman arm during the three flashing cycles of tip-blinking for the same direction again, only the current flashing cycle is completed and then the new command is processed (either three flashing cycles due to tip-blinking or constant direction blinking).

Hazard warning light. Tightly coupled with the direction blinking is the hazard warning light, which requirements are described in the following.

ELS-8 As long as the hazard warning light switch is pressed (active), all direction indicators flash synchronously. If the ignition key is in the ignition lock, the pulse ratio is bright to dark 1:1. If the ignition key is not in the lock, the pulse ratio is 1:2.

ELS-9 The adaptation of the pulse ratio must occur at the latest after two complete flashing cycles.
Note: The reduction of the pulse is performed due to energy saving reasons, such that, in case of an emergency situation, the hazard warning light is active as long as possible before the car battery is empty.

ELS-10 The duration of a flashing cycle is 1 second.

ELS-11 A flashing cycle (bright to dark) must always be completed, before a new flashing cycle can occur.
Note: By the fact, that a flashing cycle must always be completed, a "switching" behavior of the indicator is avoided. Thus, for example a change of the pitman arm from "tip-blinking" to "direction blinking" or back has no visible effect.

ELS-12 When hazard warning is deactivated again, the pitman arm is in position "direction blinking left" or "direction blinking right" ignition is On, the direction blinking cycle should be started (see Req. ELS-1).

ELS-13 If the warning light is activated, any tip-blinking will be ignored or stopped if it was started before.

Low beam headlights and **Cornering light.** The function low beam headlights includes the functions *daytime running light*, *ambient light*, and *parking light*.

ELS-14 If the ignition is On and the light rotary switch is in the position On, then low beam headlights are activated.

ELS-15 While the ignition is in position KeyInserted: if the light rotary switch is turned to the position On, the low beam headlights are activated with 50% (to save power). With additionally activated ambient light, ambient light control (Req. ELS-19) has priority over Req. ELS-15. With additionally activated daytime running light, Req. ELS-15 has priority over Req. ELS-17.

ELS-16 If the ignition is already off and the driver turns the light rotary switch to position Auto, the low beam headlights remain off or are deactivated (depending on the previous state). In case of conflict, Req. ELS-16 has priority over Req. ELS-17 (i.e. the later manual activitiy overrules running daytime light if ignition is KeyInserted). If ambient light is active (see Req. ELS-19), ambient light delays the deactivation of the low beam headlamps.

ELS-17 With activated *daytime running light*, the low beam headlights are activated after starting the engine. The daytime running light remains active as long as the ignition key is in the ignition lock (i.e. KeyInserted or KeyInIgnitionOnPosition). With additionally activated ambient light, ambient light control (Req. ELS-19) has priority over daytime running light.

ELS-18 If the light rotary switch is in position Auto and the ignition is On, the low beam headlights are activated as soon as the exterior brightness is lower than a threshold of 200 lx. If the exterior brightness exceeds a threshold of 250 lx, the low beam headlights are deactivated. In any case, the low beam headlights remain active at least for 3 seconds.

ELS-19 Ambient light prolongs (keeps low beam headlamps at 100% if they have been active before) the activation of low beam headlamps (as ambient light) if ambient light has been activated, engine has been stopped (i.e. keyState changes from KeyInIgnitionOnPosition to NoKeyInserted or KeyInserted) and the exterior brightness outside the vehicle is lower than the threshold 200 lx. In this case, the low beam headlamps remain active or are activated. The low beam headlights are deactivated or parking light is activated (see Req. ELS-28) after 30 seconds. This time interval is reset by

- Opening or closing a door
- Insertion or removal of the ignition key

ELS-20 — *Deleted requirement* —

ELS-21 With activated darkness switch (only armored vehicles) the ambient lighting is not activated. As long as the darkness switch is activated, it supresses low beam headlights due to ambient light.

ELS-22 Whenever the low or high beam headlights are activated, the tail lights are activated, too.

ELS-23 In USA or Canada, tail lights realize the direction indicator lamps. In case of direction blinking or hazard blinking, blinking has preference against normal tail lights.

ELS-24 *Cornering light*: If the low beam headlights are activated and direction blinking is requested, the cornering light is activated, when the vehicle drives slower than 10 km/h. 5 seconds after passing the corner (i.e. the direction blinking is not active any more for 5 seconds), the cornering light is switched off in a duration of 1 second (gentle fade-out). Activating cornering light means that if driving to the left is indicated, the left cornering light is activated. If driving to the right is indicated, the right cornering light shall be activated.

ELS-25 With activated darkness switch (only armored vehicles) the cornering light is not activated.

ELS-26 The cornering light is also activated, if the direction blinking is not activated, but all other constraints (see Req. ELS-24) are fulfilled and the steering wheel deflection is more than $\pm 10°$.

ELS-27 If reverse gear is activated, both opposite cornering lights are activated.

ELS-28 *Parking light.* The parking light is the low beam and the tail lamp on the left or right side of the vehicle to illuminate the vehicle if it is parked on a dark road at night. The parking light is activated, if the key is not inserted, the light switch is in position On, and the pitman arm is engaged in position left or right (②/③). To save battery charge, the parking light is activated with only 10% brightness of the normal low beam lamp and tail lamp. An active ambient light (see Req. ELS-19) delays parking light.

ELS-29 The normal brightness of low beam lamps, brake lights, direction indicators, tail lamps, cornering lights, and reverse light is 100%.

Manual high beam headlights. The low beam light is designed in such a way that it does not dazzle oncoming traffic. On country roads in particular, however, it is useful to illuminate a larger area when there is no oncoming traffic. High beam light fulfills this purpose.

ELS-30 The headlamp flasher is activated by pulling the pitman arm, i.e. as long as the pitman arm is pulled ①, the high beam headlight is activated.

ELS-31 If the light rotary switch is in position On, pushing the pitman arm to ④ causes the activation of the high beam headlight with a fixed illumination area of 220 m and 100 % luminous strength (i.e. `highBeamMotor` = 7 and `highBeamRange` = 100).

Adaptive high beam headlights. Frequent switching of the high beam is tiring for the driver. With the help of a built-in camera, which detects oncoming vehicles, this task can be automated so that the driver has better illumination of the road as often as possible without endangering oncoming traffic. In addition, the high beam headlight is optimized to always illuminate the appropriate area according to the current speed.

ELS-32 If the light rotary switch is in position Auto, the adaptive high beam is activated by moving the pitman arm to the back ④.

ELS-33 If adaptive high beam headlight is activated and the vehicle drives faster than 30 km/h and no light of an advancing vehicle is recognized by the camera, the street should be illuminated within 2 seconds according to the characteristic curve in Fig. 7 (for light illumination distance) and Fig. 8 (for luminous strength).

ELS-34 If the camera recognizes the lights of an advancing vehicle, an activated high beam headlight is reduced to low beam headlight within 0.5 seconds by reducing the area of illumination to 65 meters by an adjustment of the headlight position as well as by reduction of the luminous strength to 30%.

ELS-35 If no advancing vehicle is recognized any more, the high beam illumination is restored after 2 seconds.

ELS-36 The light illumination distance of the high beam headlight is within 100m and 300m, depending on the vehicle speed (see characteristic curve in Fig. 7).

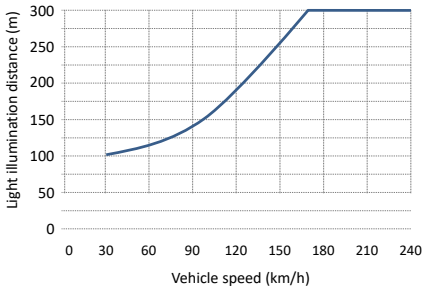

Fig. 7: Characteristic curve of the high beam headlight illumination distance depending on the vehicle speed

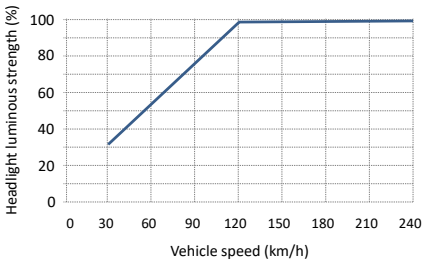

Fig. 8: Characteristic curve of the high beam headlight luminous depending on the vehicle speed

ELS-37 If an adaptive cruise control is part of the vehicle, the light illumination distance is not calculated upon the actual vehicle speed but the target speed provided by the advanced cruise control.

ELS-38 If the pitman arm is moved again in the horizontal neutral position, the adaptive high beam headlight is deactivated. The illumination of the street is reduced immediately (i.e. without gentle fade-out) to low beam headlights.

Emergency brake light. For safety reasons, it is important to indicate braking to the drivers behind the vehicle. Studies have shown that a flickering brake light during an emergency stop shortens the reaction time of the following driver.

ELS-39 If the brake pedal is deflected more than 3°, all brake lamps have to be activated until the deflection is lower than 1° again.

ELS-40 If the brake pedal is deflected more than 40.0° (i.e. full-brake application), all brake lamps flash with pulse ratio bright to dark 1:1 and a frequency of 6±1 Hz (i.e. 360±60 flashes per minute). The flashing stops only when the brake pedal is in its neutral position again (i.e. `brakePedal` = 0).

Reverse light indicates that the reverse gear in engaged, i.e. the vehicle will move backwards.

ELS-41 The reverse light is activated whenever the reverse gear is engaged.

Fault handling. A malfunctioning lighting system is safety critical and must therefore be avoided. E.g. the failure of individual lamps is checked using a hardware circuit and indicated to the driver accordingly. In the following we describe how the software should react to over- or subvoltage in order to guarantee the most important functionality for as long as possible.

ELS-42 A subvoltage is present if the voltage in the vehicle electrical system is less than 8.5V. With subvoltage, the adaptive high beam headlight is not available.

ELS-43 If the light rotary switch is in position Auto and the pitman arm is pulled, the high beam headlight is activated (see Req. ELS-31) even in case of subvoltage.

ELS-44 With subvoltage the ambient light is not available.

ELS-45 With subvoltage the cornering light is not available.

ELS-46 With subvoltage an activated parking light is switched off.

ELS-47 An overvoltage is present if the voltage in the vehicle electrical system is more than 14.5V. With overvoltage, activated lights must not exceen the maximum light intensity of $(100 - (\texttt{voltage} - 14.5) \cdot 20)\%$. This reduction serves the protection of the illuminant (protection from "burning out").

ELS-48 With overvoltage, the illumination area requirements do not need to be respected (see Req. ELS-33 and Req. ELS-36). Instead, illumination area is fixed to 220m.

ELS-49 If the camera is not Ready, adaptive high beam headlights is not available. This means, if `cameraState` is unequal Ready, light rotary switch is in position Auto and the pitman arm is in position ④, manual high beam headlights are activated (see Req. ELS-31), which means that high beam headlights are activated with a fixed illumination area of 220m and 100% luminous strength (i.e. `highBeamMotor` = 7 and `highBeamRange` = 100).

5 Speed Control System

The speed control system is a comfort function that tries to maintain or adjust the speed of the vehicle according to various external influences. In various traffic situations, this relieves the driver, who no longer has to keep the gas pedal in the corresponding position with his right foot. It includes the following user functions:

- **Cruise Control:** The vehicle automatically maintains a set speed independently of the distance to other vehicles. Here, the driver is in charge to maintain safety distance.
- **Adaptive Cruise Control:** The vehicle maintains the distance to the preceding vehicle including braking until a full standstill and starting from a standstill.
- **Distance Warning:** The vehicle warns the driver visually and/or acoustically if the vehicle is closer to the car ahead than allowed by the safety distance.
- **Emergency Brake Assist:** The vehicle decelerates in critical situations to a full standstill.
- **Speed Limit:** The vehicle does not exceed a set speed.
- **Sign Recognition:** The vehicle sets the speed limit automatically according to the recognized signs.
- **Traffic Jam Following:** The vehicle accelerates from a standstill when the preceding vehicle departs.

Similar to the exterior light system, the speed control system provides a specific user interface, uses sensors and controls actuators, which are described in the following sections.

5.1 User Interface

Cruise control lever (Fig. 9). The cruise control lever combines the functionality for the cruise control and the speed limiter. It is a little bit smaller than the pitman arm lever and is mounted below it on the steering wheel switch module. The cruise control lever also contains the rotary switch with which the safety distance can be set (see Req. SCS-24). The lever always returns to the neutral position when not touched by the user. The position of the cruise control lever is signaled via `SCSLever`.
The following movements are possible with the lever:

- By pulling towards the driver ① (Forward): The cruise control is activated with the current speed as the desired speed or the last saved desired speed.
- By moving up or down ②/③: The desired speed is increased/decreased in several steps.

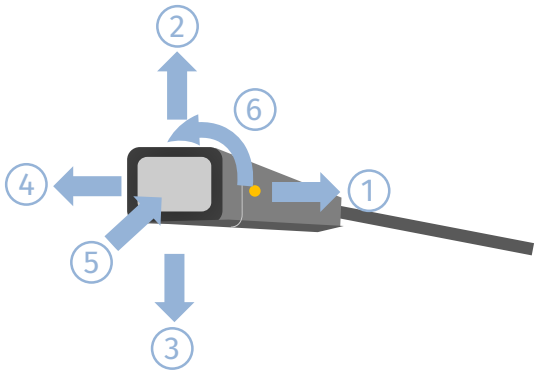

Fig. 9: Speed limiting lever integrated in the cruise control lever

- By pushing the lever away from the driver ④ (Backward): The cruise control is deactivated.
- By turning the head ⑥: The safety distance (`safetyDistance`) for the adaptive cruise control is modified in three steps (see Req. SCS-24, values 2s, 2.5s, 3s).
- The cruise control lever can be used as speed limiting lever by pushing the button at the head ⑤ of the cruise control lever. The position of the button is signalled via `speedLimiterSwitchOn`. If the lever controls the speed limit function, an orange LED integrated in the cruise control lever is on (implemented by hardware). The movements have similar functions as for the cruise control (activation, setting of the speed limit, deactivation).

Brake pedal. The brake pedal is mounted in the footwell area of the driver. Its position is signaled via `brakePedal`.

Gas pedal. The gas pedal is mounted in the footwell area of the driver. Its position is signaled via `gasPedal`.

Instrument cluster. The user can activate or deactivate the functions *traffic sign detection* and *adaptive cruise control* in the instrument cluster settings menu (which is not described in this specification). The instrument cluster settings are transmitted via `trafficSignDetectionOn` and `cruiseControlMode`.

5.2 Sensors

The following sensors are connected to the system in order to enable the driver assistance system.

- Status and position of the key (and thus the information, if the ignition is on). This information is transmitted via `keyState` and has the values NoKeyInserted, KeyInserted, KeyInIgnitionOnPosition.

- Engine status `engineOn` (True, False).
- Deflection of the brake pedal `brakePedal`, where 0 means no deflection and 225 means a maximum deflection of 45°.
- A radar system that measures the distance to the nearest obstacle. The state of the radar sensors is reported via `rangeRadarState`, its obstacle detection via `rangeRadarSensor`.

5.3 Actuators

The following actuators are controlled by the speed control system:

- The *engine* is controlled by the two inputs `gasPedal` and `setVehicleSpeed`. The engine applies the maximum of both inputs if `speedLimiterSwitchOn` = False. If `speedLimiterSwitchOn` = True, the engines applies `setVehicleSpeed` it this value is greater 0, otherwise `gasPedal`.
  Please note:
  (1) The scales of `gasPedal` and `setVehicleSpeed` are different. A maximum `gasPedal` (=45°) is equal to maximum `setVehicleSpeed`.
  (2) There is no direct relation of `gasPedal` (or `setVehicleSpeed`) to the vehicle speed. In fact, as long as `gasPedal` (or `setVehicleSpeed`) is greater 0, the vehicle accelerates. This acceleration is reduced by the inertia of the vehicle and limited by the car physics that result in a maxmimum speed of approx. 250 km/h.
  (3) The maximum acceleration is approx. 3m/s^2.
- The *brake* is controlled by the system in order to decelerate or even emergency brake if necessary via `brakePressure`. The maximum brake-implied decelaration is approx. 6m/s^2. For sake of simplicity it may be assumed that the deceleration d can be determined via `brakePedal` as

$$d = \frac{\texttt{brakePedal}}{37.5^\circ s^2/m}$$

- An *acoustic warning* and a *visual warning* are given in dangerous situations via `acousticWarningOn` and `visualWarningOn`.

5.4 Software Functions

Setting and modifying desired speed This section describes how to set and modify the desired speed both for adaptive cruise control and (normal) cruise control. When changing the desired speed, the instrument cluster displays the current value. This is not covered in this specification.

SCS-1 After engie start, there is no previous desired speed. The valid values for desired speed are from 1 km/h to 200 km/h.

SCS-2 When pulling the cruise control lever to ①, the desired speed is either the current vehicle speed (if there is no previous desired speed) or the previous desired speed (if already set).

SCS-3 If the current vehicle speed is below 20km/h and there is no previous desired speed, then pulling the cruise control lever to ① does not activate the (adaptive) cruise control.

SCS-4 If the driver pushes the cruise control lever to ② up to the first resistance level (5°) and the (adaptive) cruise control is activated, the desired speed is increased by 1 km/h.

SCS-5 If the driver pushes the cruise control lever to ② above the first resistance level (7°, beyond the pressure point) and the (adaptive) cruise control is activated, the desired speed is increased to the next ten's place.

Example: Current desired speed is 57 km/h ⟶ new desired speed is 60 km/h.

SCS-6 Pushing the cruise control lever to ③ reduces the desired speed accordingly to Req. SCS-4 and Req. SCS-5. The lowest desired speed that can be set by pushing the cruise control lever beyond the pressure point is 10 km/h.

SCS-7 If the driver pushes the cruise control lever to ② with activated cruise control within the first resistance level (5°, not beyond the pressure point) and holds it there for 2 seconds, the desired speed of the cruise control is increased every second by 1 km/h until the lever is in neutral position again.
Example: Current desired speed is 57 km/h ⟶ new desired speed is 58 km/h (due to Req. SCS-4), after holding 2 seconds, desired speed is set to 59 km/h, after holding another second, desired speed is set to 60 km/h, after holding another second, desired speed is set to 61 km/h, etc.

SCS-8 If the driver pushes the cruise control lever to ② with activated cruise control through the first resistance level (7°, beyond the pressure point) and holds it there for 2 seconds, the speed set point of the cruise control is increased every 2 seconds to the next ten's place until the lever is in neutral position again.
Example: Current desired speed is 57 km/h ⟶ new desired speed is 60 km/h (due to Req. SCS-5), after holding 2 seconds, desired speed is set to 70 km/h, after another 2 seconds, desired speed is set to 80 km/h, after holding another 2 seconds, desired speed is set to 90 km/h, etc.

SCS-9 If the driver pushes the cruise control lever to ③ with activated cruise control within the first resistance level (5°, not beyond the pressure point) and holds it there for 2 seconds, the desired speed of the cruise control is reduced every second by 1 km/h until the lever is in neutral position again.
Example: Current desired speed is 57 km/h ⟶ new desired speed is 56 km/h (due to Req. SCS-6) after holding 2 seconds,desired speed is set to 55 km/h, after another second, desired speed is set to 54 km/h, after holding another second, desired speed is set to 53 km/h, etc.

SCS-10 If the driver pushes the cruise control lever to ③ with activated cruise control through the first resistance level (7°, beyond the pressure point) and holds it there for 2 seconds, the speed set point of the cruise control is increased every 2 seconds to the next ten's place until the lever is in neutral position again.

SCS-11 If the (adaptive) cruise control is deactivated and the cruise control lever is moved up or down (either to the first or above the first resistance level, the current vehicle speed is used as desired speed.

SCS-12 Pressing the cruise control lever to ④ deactivates the (adaptive) cruise control. `setVehicleSpeed` = 0 indicates to the car that there is no speed to maintain.

Cruise Control The following requirements describe the simple cruise control system without adaption to the traffic situation which is the basis for the adaptive cruise control system. The distinction between cruise control and adaptive cruise control is made via `cruiseControlMode`.

SCS-13 The cruise control is activated using the cruise control lever according to Reqs. SCS-1 to SCS-12.

SCS-14 As long as the cruise control is activated, the vehicle maintains the current vehicle speed at the desired speed without the driver having to press the gas pedal or the brake pedal.

SCS-15 If the driver pushes the gas pedal and by the position of the gas pedal more acceleration is demanded than by the cruise control, the acceleration setting as demanded by the driver is adopted.
Note: This handling is done by the engine autonomously.

SCS-16 By pushing the brake, the cruise control is deactivated until it is activated again.

SCS-17 By pushing the control lever backwards, the cruise control is deactivated until it is activated again.

Adaptive Cruise Control In the adaptive cruise control mode, maintenance of the speed does not only depend on the desired speed but also vehicles ahead. For this purpose, the desired speed of the driver must be distinguished from the target speed of the control system. The Reqs. SCS-13 to SCS-17 still hold except

SCS-14. The distinction between cruise control and adaptive cruise control is made via `cruiseControlMode`.

SCS-18 When the driver enables the cruise control (by pulling the cruise control lever or by pressing the cruise control lever up or down), the vehicle maintains the set speed if possible.

SCS-19 The adaptive cruise control desired speed is controlled using the cruise control lever according to Reqs. SCS-1 to SCS-12.

SCS-20 If the distance to the vehicle ahead falls below the specified speed-dependent safety distance (see Req. SCS-24), the vehicle brakes automatically. The maximum deceleration is 3m/s^2.

SCS-21 If the maximum deceleration of 3m/s^2 is insufficient to prevent a collision with the vehicle ahead, the vehicle warns the driver by two acoustical signals (0.1 seconds long with 0.2 seconds pause between) and by this demands to intervene.

SCS-22 If the distance to the preceding vehicle increases again above the speed-dependent safety distance, the vehicle accelerates with a maximum of 1m/s^2 until the set speed is reached.

Example: Figure 10 shows an exemplary situation with a desired speed of 120 km/h. At the beginning, the car drives at this speed until another car appears with 80 km/h. The adaptive cruise control decelerates to 80 km/h with a maximum deceleration of 3m/s^2. If this is not sufficient, two acoustical signals warn the driver. As soon as the vehicle in front accelerates to 100 km/h, the adaptive cruise control also accelerates with a maximum of 1m/s^2. When the vehicle in front finally accelerates to a speed of more than 120 km/h the adaptive cruise control increases the speed back to 120 km/h.

SCS-23 If the speed of the preceding vehicle is 20 km/h or below, the distance is set to $2.5\text{s} \cdot$ `currentSpeed`, down to a standstill. When both vehicles are standing the absolute distance is regulated to 2m. When the preceding vehicle is accelerating again, the distance is set to $3\text{s} \cdot$ `currentSpeed`. This distance is valid until the vehicle speed exceeds 20 km/h, independent of the user's input via the distance level (turning the cruise control lever head).

SCS-24 By turning the cruise control lever head, the distance to be maintained to the vehicle ahead can be selected. Three levels are available: 2 seconds, 2.5 seconds and 3 seconds. The desired level only applies within the velocity window > 20 km/h. Below this level, the system autonomously sets the distance according to Req. SCS-23.

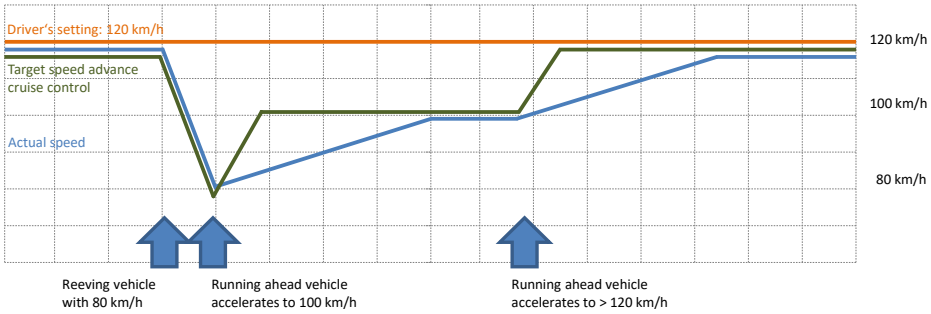

Fig. 10: Illustration of the difference between "actual speed", "desired speed", and "target speed" of the adaptive cruise control

Distance warning. The adaptive cruise control system has to calculate the distance (time) to the vehicle ahead and has to issue the following warnings depending on the calculated value:

SCS-25 A visual warning is activated if the actual distance is less than $(\textit{current speed}/3.6) \cdot 1.5$.

SCS-26 An acoustic alarm is activated if the actual distance is less than $(\textit{current speed}/3.6) \cdot 0.8$.

Emergency Brake Assistant. The emergency brake assistant initiates braking in critical situations.

SCS-27 The emergency brake assistant must be available in the following speed windows: 0 - 60 km/h, for emergency braking to stationary obstacles, 0 – 120 km/h on moving obstacles.

SCS-28 The time necessary to perform braking to standstill is determined by the value for the maximum deceleration. If an object is ahead of the vehicle and the time until an impact is less or equal to the time until a standstill plus 3 seconds, three acoustic signals are given (0.1 seconds long with 0.05 seconds pause between) is issued and the brakes are activated by 20% (i.e. 1.2m/s^2). If the time until an impact is less or equal to the time until a standstill plus 1.5 seconds, the brake is activated by 60% (i.e. 3.6m/s^2. If the time until an impact is less or equal to the time until standstill then the brake is activated at 100% (i.e. 6m/s^2). In case that both adaptive cruise control (see Req. SCS-20) and the emergency brake assistand request braking, the higher deceleration value shall be applied.

Speed Limit. The speed limit function prevents the driver from accidentally driving faster than a preset desired speed. In case of emergency, the driver can overrule the speed limit.

SCS-29 The speed limiter mode is activated by pressing the button at the head of the control lever.

SCS-30 An active speed limit function of the cruise lever is indicated by an orange LED integrated in the control lever (realized in hardware).

SCS-31 Activating speed limit desired speed and modifying the desired speed is done according to Reqs. SCS-1 to SCS-12.

SCS-32 As long as the speed limit function is activated, the current speed must not exceed the set speed limit.

SCS-33 By pressing the gas pedal beyond 90% the speed limit is temporarily deactivated.

SCS-34 When the pressure on the gas pedal decreases below 90%, the speed limit is automatically activated again.

SCS-35 An active speed limit can be deactivated by either pushing the cruise control lever backwards ④ or by pushing the head of the cruise control lever ⑤.

Traffic Sign Detection If a road sign is indicating a speed limit with active traffic sign detection (controlled by `trafficSignDetectionOn`), the desired speed is modified by the recognized traffic sign value.

SCS-36 Traffic sign detection is active, while adaptive cruise control is active and the driver has activated traffic sign detection in the instrument cluster.

SCS-37 With active traffic sign detection and gas pedal in position 0, a recognized traffic sign sets the desired speed to the detected value.

SCS-38 A later manual modification of the desired speed via the cruise control lever (see Reqs. SCS-1 to SCS-12) modifies the desired speed again. Hint: The desired speed is determined by the latest modification: A user setting via cruise control lever is overruled by a later traffic sign detection and this is again overruled by a later modification via cruise control lever.

SCS-39 If traffic sign detection recognizes Unlimited, the new desired speed is set to

- 120 km/h, if the previous desired speed has been lower than 120 km/h
- the desired speed d_{man}, where d_{man} is the last manually set desired speed that has been higher than 120 km/h

Note: For the sake of simplicity, country dependence and road type dependence has been omitted.

Fault handling and general properties A malfunctioning speed control system might be safety critical and must therefore be avoided. E.g. a wrong detection of the distance to the car in front could lead to dangerous situations. These situations should be avoided with the following requirements.

SCS-40 The radar system carries out a self-test at each start and also continuously checks the plausibility of the values of the various sensors. If one of the values is found to be extremely close, the status is set to "Dirty". During the self-test and with other errors (strong fluctuations, very different values of the individual sensors) the status is set to "NotReady".

SCS-41 If the radar sensor self-test device reports a fault (Dirty or NotReady), all systems depending on the distance to the vehicle must be suspended and the driver must be warned by an appropriate light in the instrument cluster (not part of this specification). In this case, the self-test of the radar system is restarted every 10 min.

SCS-42 The gas or brake pedal depressed by the driver must always be able to override a target speed specified by the system.

SCS-43 If the system performs a brake action, the brake lights must be activated as if the brake pedal has been pressed by the driver (see light system specification).

References

1. Boniol, F., Wiels, V.: The Landing Gear System Case Study. In: Boniol, F., Wiels, V., Ait Ameur, Y., Schewe, K.D. (eds.) ABZ 2014: The Landing Gear Case Study. pp. 1–18. Springer International Publishing, Cham (2014)

2. Hoang, T.S., Butler, M., Reichl, K.: The Hybrid ERTMS/ETCS Level 3 Case Study. In: Butler, M., Raschke, A., Hoang, T.S., Reichl, K. (eds.) Abstract State Machines, Alloy, B, TLA, VDM, and Z. pp. 251–261. Springer International Publishing, Cham (2018)
3. Houdek, F.: Automotive Example: Exterior Lighting and Speed Control. In: Pohl, K., Broy, M., Daembkes, H., Hönninger, H. (eds.) Advanced Model-Based Engineering of Embedded Systems, pp. 13–19. Springer International Publishing (2016)
4. Mashkoor, A.: The Hemodialysis Machine Case Study. In: Butler, M., Schewe, K.D., Mashkoor, A., Biro, M. (eds.) Abstract State Machines, Alloy, B, TLA, VDM, and Z. pp. 329–343. Springer International Publishing, Cham (2016)

A Interface

The following table defines all signals that either reflect the determined input of the various user interfaces and sensors or are used to control the actuators. For the sake of simplicity, all signals are available all the time. There are no timeouts or delays.

Signal identifier	**Description**	**Value range**
`keyState`	Status of ignition key	NoKeyInserted, KeyInserted, KeyInIgnitionOnPosition
`engineOn`	Status of engine	True, False
`allDoorsClosed`	Status of vehicle doors	True, False
`gasPedal`	Deflection of the gas pedal from the neutral position	Resolution: 0.2° Value range: 0–225 (0.0–45.0°)
`brakePedal`	Deflection of the brake pedal from the neutral position	Resolution: 0.2° Value range: 0–225 (0.0–45.0°)
`reverseGear`	Status of the reverse gear	True, False
`voltageBattery`	Available battery voltage	Resolution: 0.1 V Value range: 0–500 (0.0–50.0 V)
`currentSpeed`	Current vehicle speed in km/h	Resolution: 0.1 km/h Value range: 0–5000 (0.0–500.0 km/h)
`steeringAngle`	Steering angle (deflection of the steering wheel)	0 = sensor is calibrating 1–410 = steering wheel rotation to the left (Resolution: 1° starting from 10° deflection) 411–510 = steering wheel rotation to the left (Resolution: 0.1° for 0°–10° deflection) 511–513 = steering wheel in neutral position 514–613 = steering wheel rotation to the right (Resolution: 0.1° for 0°–10° deflection) 614–1022 = steering wheel rotation to the right (Resolution: 1° starting from 10° deflection)

Signal identifier	Description	Value range
daytimeLights	True, if option is selected in instrument cluster	True, False
ambientLighting	True, if option is selected in instrument cluster	True, False
lightRotarySwitch	Status of light rotary switch	Off, Auto, On
pitmanArmForthBack	Status of pitman arm regarding high beam (horizontal position)	Neutral, Backward, Forward
pitmanArmUpDown	Status of pitman arm regarding blinker (vertical position)	Neutral, Downward5, Downward7, Upward5, Upward7
hazardWarning-SwitchOn	Status hazard warning switch	True, False
darknessMode-SwitchOn	Status darkness switch (only armored vehicles)	True, False
brightnessSensor	Measurement of rain/light sensor regarding brightness	Resolution: 1 lx Value range: 0–100000
cameraState	Status of camera	Ready, Dirty, NotReady
oncomingTraffic	Advancing vehicle detected	True, False
brakeLight	Brake light command	0–100%
blinkLeft	Perform left blinking	0–100%
blinkRight	Perform right blinking	0–100%
lowBeamLeft	Low beam command left	0–100%
lowBeamRight	Low beam command right	0–100%
taillampleft	Tail lamp command left	0–100%
taillampright	Tail lamp command right	0–100%
highBeamOn	High beam command	True, False
highBeamRange	High beam light range (brightness)	0–300 desired light range
highBeamMotor	Desired position for high beam motor	0–14 desired position: 0 = 65 m 1 = 100m 2–14 = 120–360 m (20m step size)
corneringLightLeft	Cornering light left	0–100%
corneringLightRight	Cornering light right	0–100%
reverseLight	Reverse light command	0–100%
SCSLever	Position of cruise control lever	Neutral, Downward5, Downward7, Upward5, Upward7, Forward, Backward
safetyDistance	Safety distance level (turning knob at SCSLever)	2s, 2.5s, 3s
speedLimiterSwitchOn	Status speed limiter switch	True, False

Signal identifier	Description	Value range
rangeRadarState	status of long-range radar sensors	Ready, Dirty, NotReady
rangeRadarSensor	Evaluation of long-range radar sensor	0 = no dectected obstacle in the travel corridor 1–200 = distance in meters of obstacle detected in the travel corridor 255 = radar state is Dirty or NotReady
cruiseControlMode	Operation mode of cruise control	1 = (normal) cruise control, 2 = adaptive cruise control
trafficSign-DetectionOn	Operation mode of traffic sign detection	True, False
detectedTrafficSign	Speed limit of observed traffic sign	None, 20–130, Unlimited
setVehicleSpeed	Used to control the engine via cruise control	0–100
brakePressure	The pressure of the brake shoes	0–100%
acousticWarningOn	Acoustic warning command	True, False
visualWarningOn	Visual warning command	True, False
driverPosition	Vehicle configuration of driver position	LeftHandDrive, RightHandDrive
armoredVehicle	True, if vehicle is armored	True, False
marketCode	The market region for which the car is built for	001 = USA, 002 = Canada, 003 = EU, ...