Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0
08/04/2018

Document history

Date	Version	Editor	Description
08/04/2018	1.0	GRANIE Guillaume	First Attempt

Table of Contents

Purpose of the Technical Safety Concept

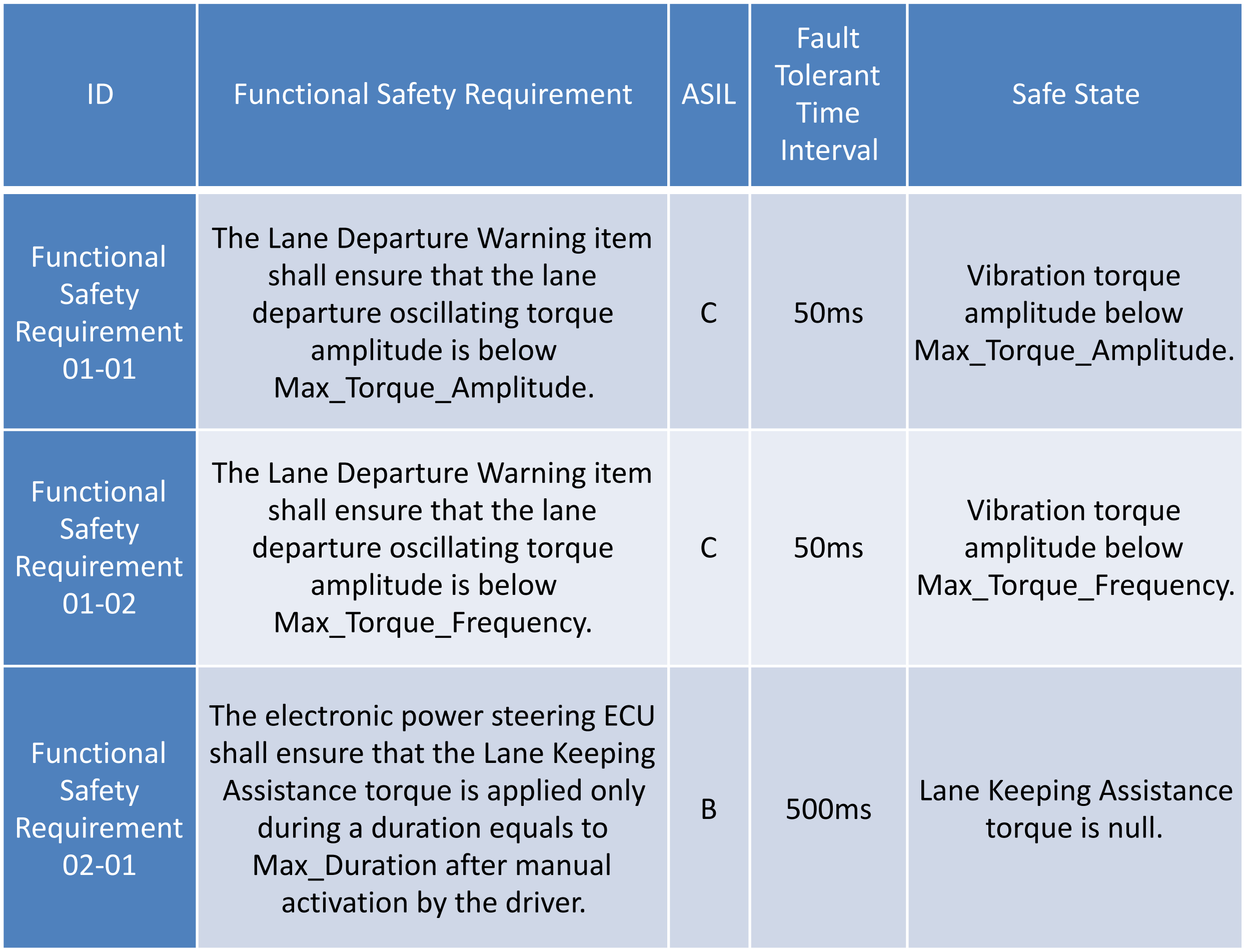
Technical safety requirements describes what a system will do when a malfunction violates a safety goal.

The technical safety concept is a level deeper into the details of the system. It has knowledge of how the system is implemented.

The Technical Safety Requirements are derived directly from the Functional Safety Requirements.

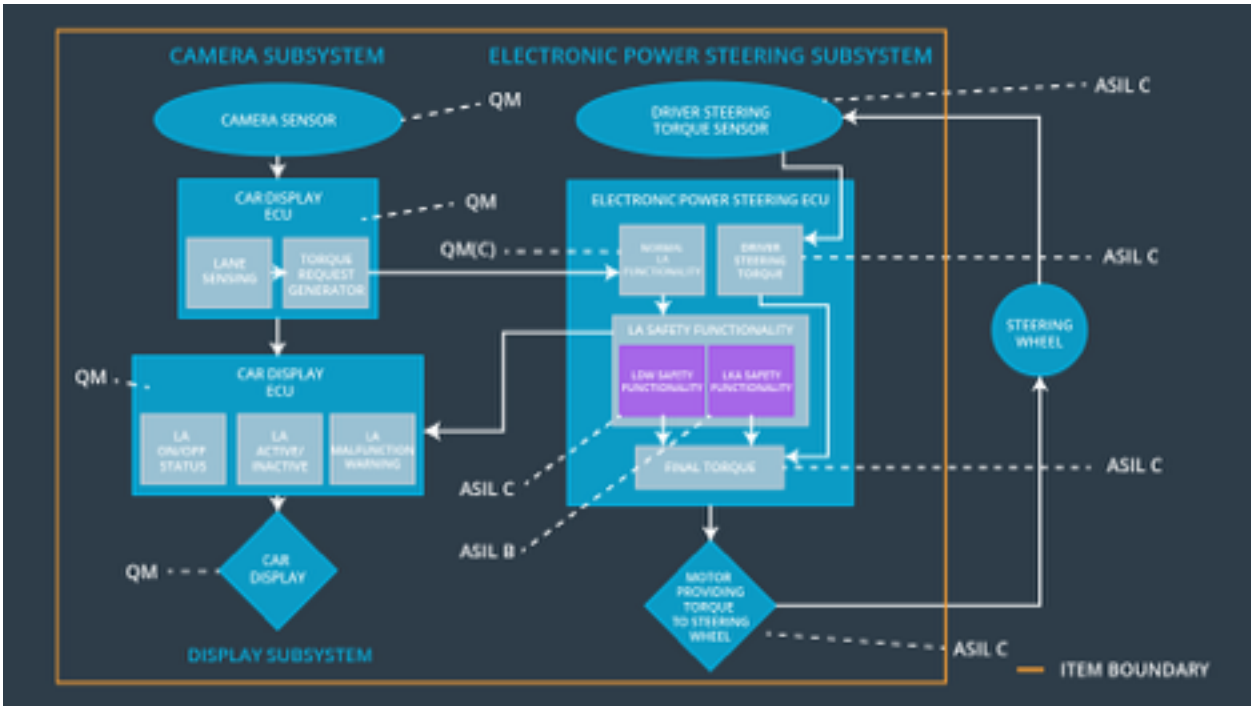
Inputs to the Technical Safety Concept

Functional Safety Requirements



ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	C	50ms	Vibration torque amplitude below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only during a duration equals to Max_Duration after manual activation by the driver.	B	500ms	Lane Keeping Assistance torque is null.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Forward facing sensor collecting images being sent to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Image processing element responsible for detecting the lane lines on the road and providing the results to the Torque Request Generator Software Component in the same Camera Sensor ECU.
Camera Sensor ECU - Torque Request Generator	Processing element responsible for converting the detected lane lines provided by the Lane Sensing element into a torque request to steer the vehicle into ego lane. This request will be sent to the Electronic Power Steering ECU.
Car Display	Screen responsible for displaying informational and warning messages to the driver.

Element	Description
Car Display ECU - Lane Assistance On/Off Status	Processing element responsible for displaying on the car display element the status, either ON or OFF, of the Lane Assistance functionality.
Car Display ECU - Lane Assistant Active/Inactive	Processing element responsible for indicating whether the Lane Assistance functionality is properly (Active) or improperly (Inactive) functioning.
Car Display ECU - Lane Assistance malfunction warning	Processing element responsible for indicating on the car display element any detected malfunction of the Lane Assistance functionality.
Driver Steering Torque Sensor	Sensor responsible for measuring the amount of torque applied by the driver to the steering wheel in both rotational directions.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processing unit responsible for converting the torque sensed on the steering wheel applied by the driver and convert it into the appropriate steering of the vehicle.
EPS ECU - Normal Lane Assistance Functionality	Processing unit responsible for converting the torque request received from the Torque Request Generator inside the Camera Sensor ECU into an appropriate torque signal to the steering motor.
EPS ECU - Lane Departure Warning Safety Functionality	Software Component responsible for ensuring that the provided torque request from the Lane Assistance functionality has an amplitude below Max_Torque_Amplitude and a torque frequency below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software Component responsible for ensuring that the Lane Keeping Assistant Functionality is never activated longer than Max_Duration.
EPS ECU - Final Torque	Software Component responsible for merging the torque request from both the Lane Keeping Assistant Functionality and the Lane Departure Warning Functionality into one single signal sent to the motor.
Motor	Actuator responsible for issuing torque to the steering wheel.

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements
(derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	X		

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:

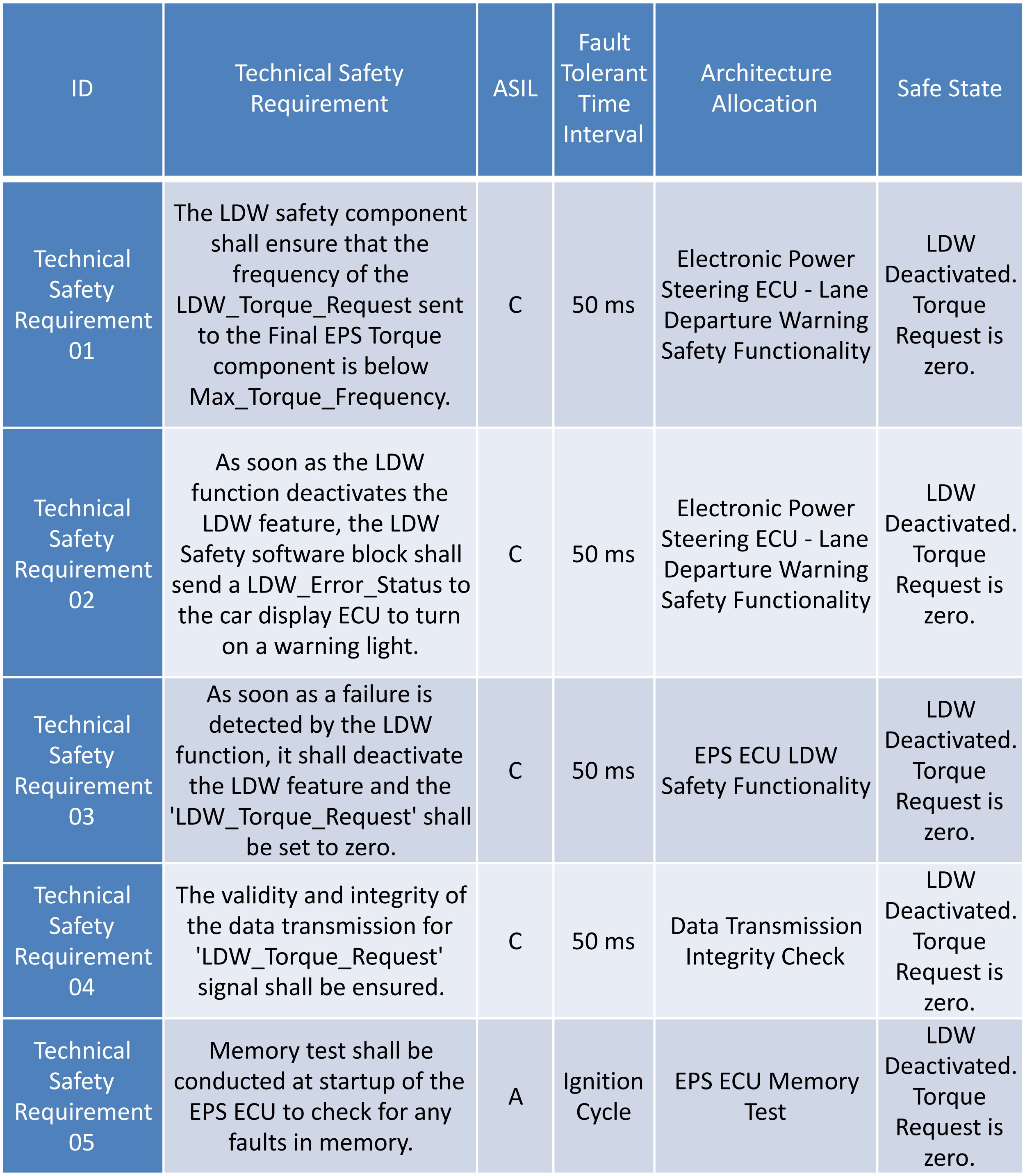
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final EPS Torque component is below Max_Torque_Amplitude.	C	50 ms	Electronic Power Steering ECU - Lane Departure Warning Safety Functionality	LDW Deactivated. Torque Request is zero.

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a LDW_Error_Status to the car display ECU to turn on a warning light.	C	50 ms	Electronic Power Steering ECU - Lane Departure Warning Safety Functionality	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	EPS ECU LDW Safety Functionality	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	EPS ECU Memory Test	LDW Deactivated. Torque Request is zero.

Functional Safety Requirement 01-2 with its associated system elements
(derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:



ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LDW safety component shall ensure that the frequency of the LDW_Torque_Request sent to the Final EPS Torque component is below Max_Torque_Frequency.	C	50 ms	Electronic Power Steering ECU - Lane Departure Warning Safety Functionality	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the LDW Safety software block shall send a LDW_Error_Status to the car display ECU to turn on a warning light.	C	50 ms	Electronic Power Steering ECU - Lane Departure Warning Safety Functionality	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	EPS ECU LDW Safety Functionality	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LDW Deactivated. Torque Request is zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	EPS ECU Memory Test	LDW Deactivated. Torque Request is zero.

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

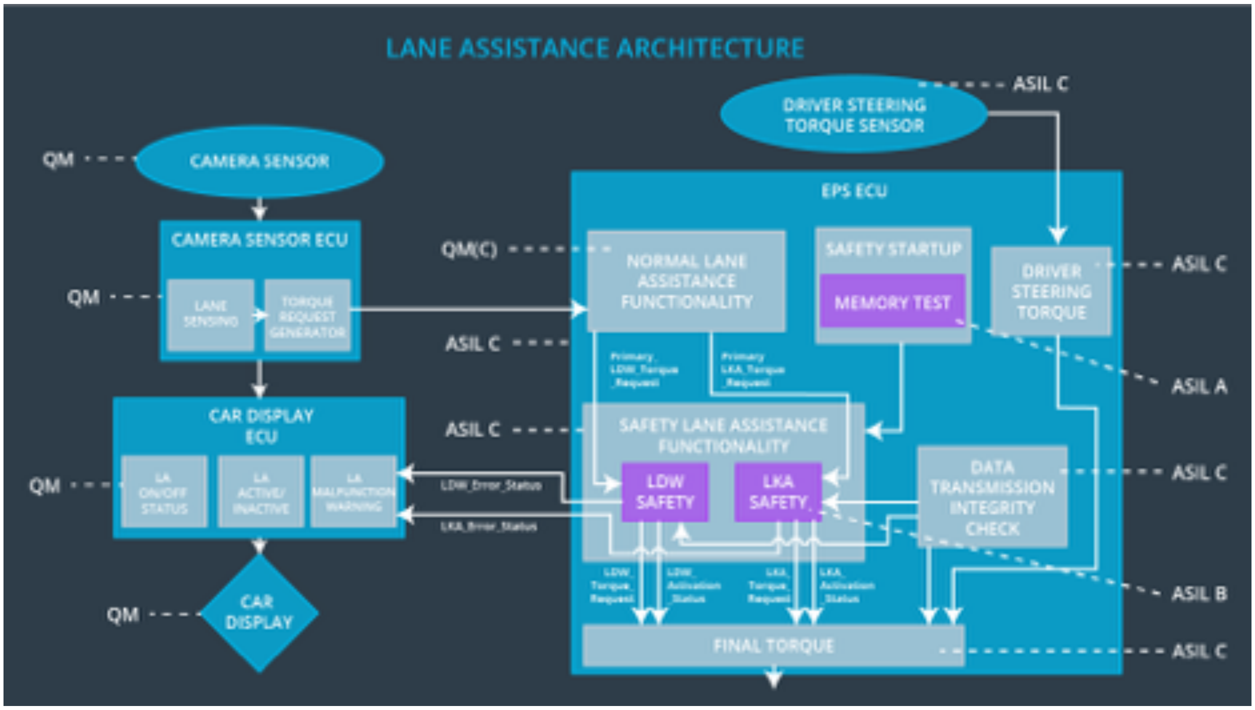
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	The LKA Safety component shall ensure that the time elapsed following the receipt of an LKA_Torque_Request from the Normal Lane Assistance Functionality component is below Max_Duration.	C	500 ms	Electronic Power Steering ECU - Lane Keeping Assistance Safety Functionality	LKA Deactivated. Torque Request is zero.
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the LKA Safety software block shall send a LKA_Error_Status to the car display ECU to turn on a warning light.	C	500 ms	Electronic Power Steering ECU - Lane Keeping Assistance Safety Functionality	LKA Deactivated. Torque Request is zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	C	500 ms	Electronic Power Steering ECU - Lane Keeping Assistance Safety Functionality	LKA Deactivated. Torque Request is zero.

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	Electronic Power Steering ECU - Lane Keeping Assistance Safety Functionality	LKA Deactivated. Torque Request is zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	EPS ECU Memory Test	LKA Deactivated. Torque Request is zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02	Yes	Dashboard signal
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Dashboard signal