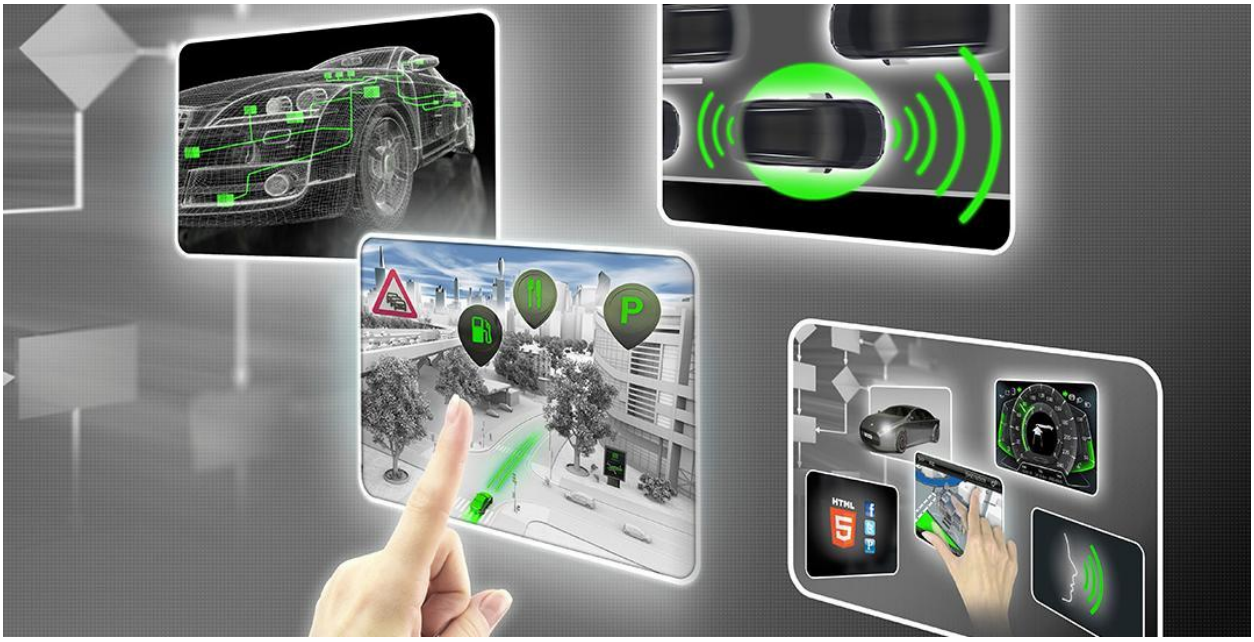


Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-06-18	1.0	H. Kube	Initial version
2018-06-21	1.1	H. Kube	Include results of review: Change the safe state of LDW and LKA to set the the torque to 0 instead of switching off the system

Table of Contents

Purpose of the Technical Safety Concept

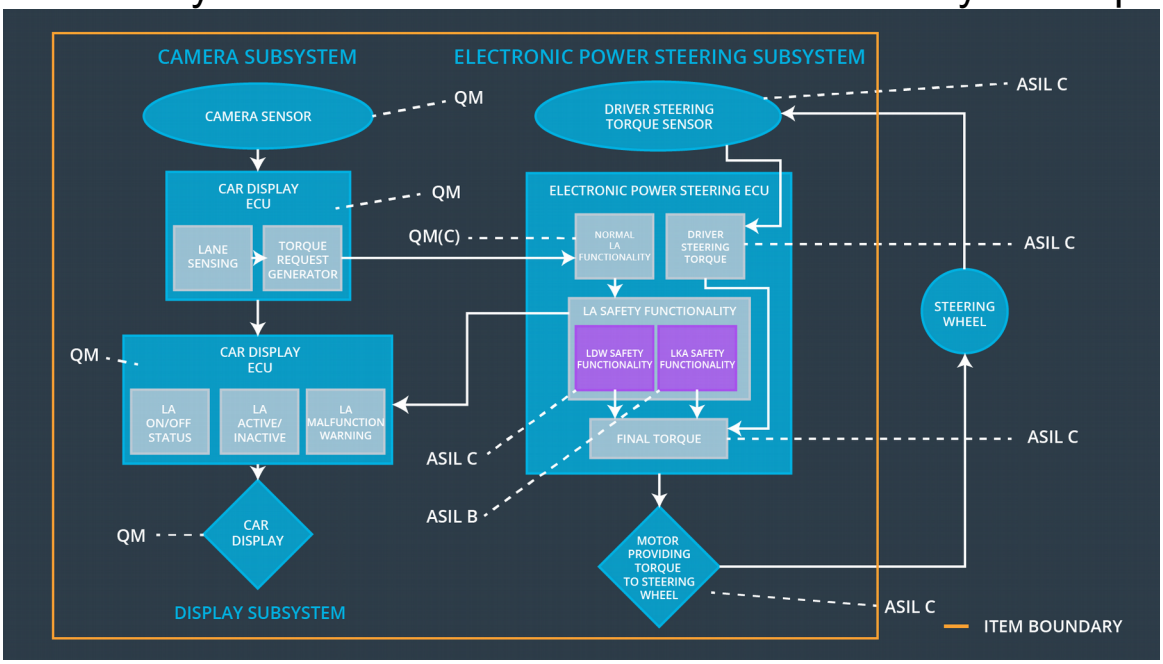
The purpose of the Technical Safety Concept is to refine the Functional Safety Requirements established in the Functional Safety Concept and allocate them to the system architecture.

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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	The LDW_Torque_Amplitude is set to 0 and a warning is displayed on the dashboard.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	The LDW_Torque_Frequency is set to 0 and a warning is displayed on the dashboard.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	The LKA_Torque is set to 0 and a warning is display on the dashboard.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures road images and provides them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detects lane markings in the road image
Camera Sensor ECU - Torque request generator	Generates a torque request to the Electronic Power Steering ECU
Car Display	Shows the driver the lane keeping assistance warning and status.
Car Display ECU - Lane Assistance On/Off Status	Indicates whether Lane Assistance is on
Car Display ECU - Lane Assistant Active/Inactive	Indicates whether Lane Assistant is active
Car Display ECU - Lane Assistance malfunction warning	Indicates whether the system is malfunctioning.
Driver Steering Torque Sensor	Measures the torque applied by the driver to the wheel.

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes the measurement result of the Driver Steering Torque sensor.
EPS ECU - Normal Lane Assistance Functionality	Receives the torque request from the Camera Sensor ECU.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the torque amplitude and the torque frequency are below their limits.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the torque is applied no longer than the Max_Duration_Time.
EPS ECU - Final Torque	Combines the torque request from LDW and LKA and sends it to the motor.
Motor	Applies the torque requested by the Electronic Power Steering ECU to the 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 Electronic Power Steering Torque' component is below 'Max_Torque_Amplitude'.	C	50 ms	LDW Safety	Signal LDW_Activation_Status is cleared
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECE to turn on a warning light.	C	50 ms	LDW Safety	Signal LDW_Error_Status is set
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature an the 'LDW_Torque_request' shall be set to zero.	C	50 ms	LDW Safety	LDW_Torque_Request is 0
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_Activation_Status is cleared, LDW_Error_Status is set and LDW_Torque_Request is 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW_Activation_Status is cleared, LDW_Error_Status is set and LDW_Torque_Request is 0

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 Electronic Power Steering Torque' component is below 'Max_Torque_Frequency'.	C	50 ms	LDW Safety	Signal LDW_Activation_Status is cleared
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECE to turn on a warning light.	C	50 ms	LDW Safety	Signal LDW_Error_Status is set
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature an the 'LDW_Torque_request' shall be set to zero.	C	50 ms	LDW Safety	LDW_Torque_Request is 0
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_Activation_Status is cleared, LDW_Error_Status is set and LDW_Torque_Request is 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW_Activation_Status is cleared, LDW_Error_Status is set and LDW_Torque_Request is 0

Lane Keeping Assistance (LKA) Requirements:

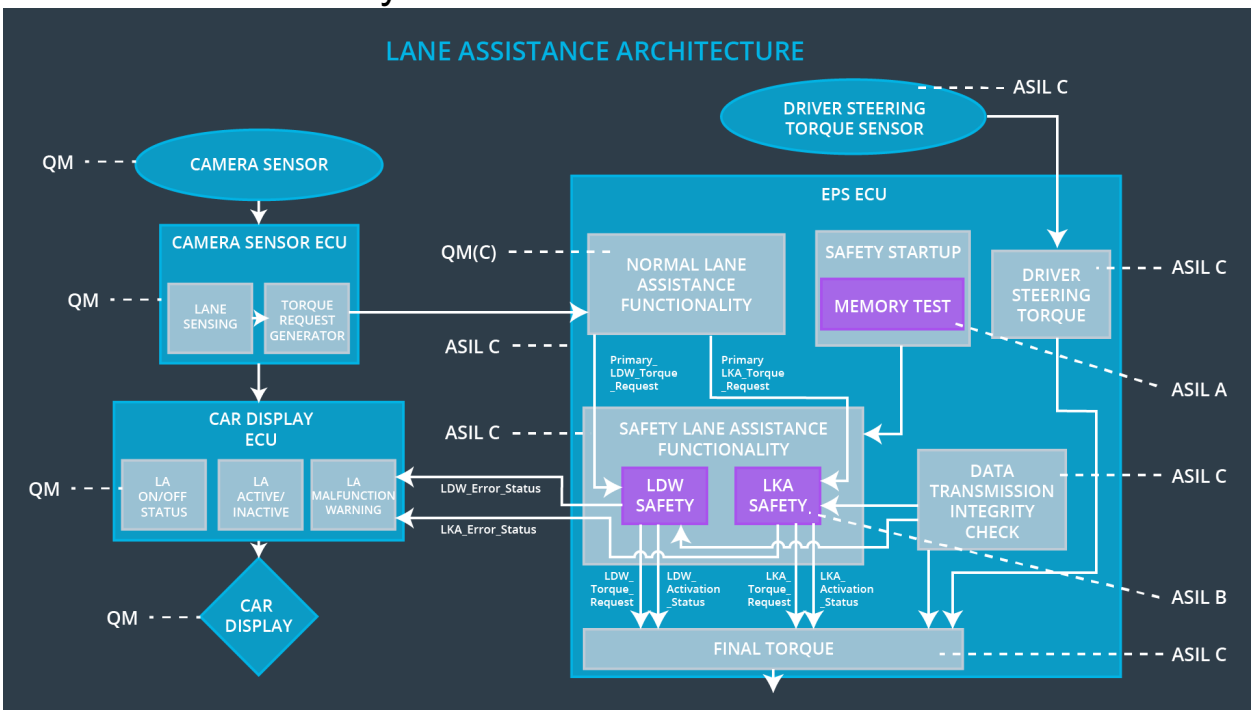
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

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	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the duration of the 'LKA_Torque_Request' sent to the 'Final Electronic Power Steering Torque' component is below 'Max_Duration'.	B	500 ms	LKA Safety	Signal LKA_Activation_Status is cleared
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECE to turn on a warning light.	B	500 ms	LKA Safety	Signal LKA_Error_Status is set
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature an the 'LKA_Torque_request' shall be set to zero.	B	500 ms	LKA Safety	LKA_Torque_Request is 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	LKA_Activation_Status is cleared, LKA_Error_Status is set and LKA_Torque_Request is 0
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LKA_Activation_Status is cleared, LKA_Error_Status is set and LKA_Torque_Request is 0

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements described in this document are allocated to the Electronic Power Steering ECU. For exact allocation refer to the tables above.

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, Malfunction_05	Yes	Lane Departure Warning indicator on car display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_04	Yes	Lane Keeping Assistance Malfunction indicator on car display