Technical Safety Concept Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
01/04/2019	1.0	Chris Sketch	Initial Documentation
01/05/2019	2.0	Chris Sketch	Add Functional Safety Concept 01-03

Table of Contents

Purpose of the Technical Safety Concept

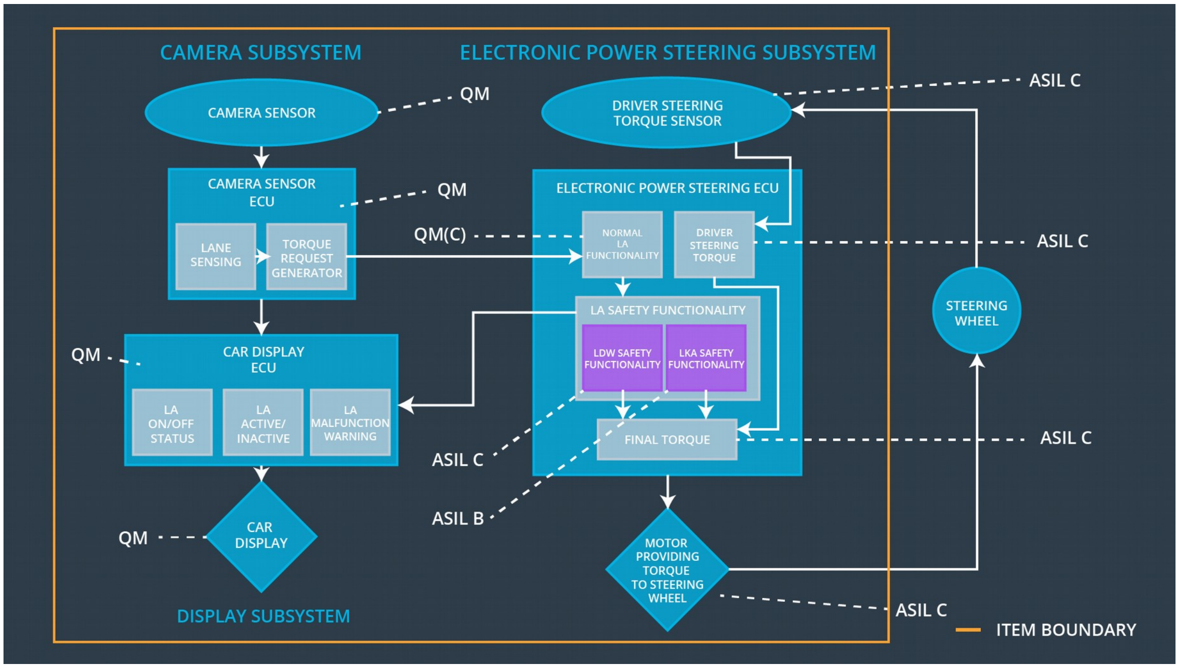
The purpose of a technical safety concept is to tie functional safety concepts to components of a system such as the sensors, control units, and actuators.

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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane departure torque is set to 0.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Lane departure torque is set to 0.
Functional Safety Requirement 01-03	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is above Min_Torque_Frequency	B	50 ms	Lane departure torque is set to 0.
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	Lane assistance torque is set to 0.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Senses visual information in the environment such as the lane markings and geometry of the road to be processed by the camera sensor ECU
Camera Sensor ECU - Lane Sensing	Processes information received from the camera sensor to determine the current lane and the vehicles position in the lane.
Camera Sensor ECU - Torque request generator	Sends request to electronic power steering ECU to steer the vehicle towards the center of the lane for lane keeping assistance function. Sends request to electronic power steering ECU that the vehicle is exiting the lane for lane departure warning function.
Car Display	Displays an icon to the driver to indicate that the vehicle is departing the lane or the lane keeping function is activated
Car Display ECU - Lane Assistance On/ Off Status	Receives request from the camera sensor ECU and displays an icon when lane assistance is on.
Car Display ECU - Lane Assistant Active/Inactive	Checks the status of lane assistance malfunction warning. Displays lane assistant inactive message when the system is malfunctioning.
Car Display ECU - Lane Assistance malfunction warning	Reads LDW_Error_Status from LDW Safety Functionality. If LA Malfunction Warning is reporting a malfunction, the LA Active/Inactive will be triggered.
Driver Steering Torque Sensor	Senses the torque that is being applied to the steering wheel. The sensor is necessary to steer and add torque in a controlled manner.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives information from the driver steering torque sensor.
EPS ECU - Normal Lane Assistance Functionality	Receives torque request from camera sensor ECU. Processes lane keeping assistance requests to determine the amount of torque necessary to steer the vehicle to the center of the lane. Sends torque request to Lane Assistance Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	Checks whether the torque Primary_LDW_Torque_Request amplitude is less

	than Max_Torque_Amplitude and frequency is less than Max_Torque_Frequency. Sets torque to 0 if it is and sends a message to the car display ECU that lane assistance is malfunctioning.
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks whether torque has been applied for longer than Max_Duration, deactivates lane assistance if it has, and sends a message to the car display ECU to indicate lane assistance is malfunctioning.
EPS ECU - Final Torque	Activates the motor providing torque to the steering wheel in order to oscillate the steering wheel using a combination of driver steering torque and LDW_Torque_Request. Activates the motor providing torque to the steering wheel in order to steer to the center of the lane
Motor	Provides torque to the steering wheel in order to alert the driver that they are exiting the lane Provides torque to the steering wheel in order to steer the vehicle to the center of the lane

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements

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	The LDW safety component shall ensure that the	C	50 ms	EPS ECU - Lane	Lane departure

Requirement 01	amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.			Departure Warning Safety Functionality	torque is set to 0.
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 ECU to turn on a warning light.	C	50 ms	EPS ECU - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
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 - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	EPS ECU – Data Transmission Integrity Check	N/A
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	EPS ECU – Memory Test	N/A

Functional Safety Requirement 01-02 with its associated system elements

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	A	Fault	Architecture	Safe

		SIL	Tolerant Time Interval	Allocation	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	EPS ECU - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
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 ECU to turn on a warning light.	C	50 ms	EPS ECU - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
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 - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	EPS ECU – Data Transmission Integrity Check	N/A
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	EPS ECU – Memory Test	N/A

Functional Safety Requirement 01-03 with its associated system elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-03	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is above Min_Torque_Frequency	B	50 ms	Lane departure torque is set to 0.

Technical Safety Requirements related to Functional Safety Requirement 01-03 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 above 'Min_Torque_Frequency.	B	50 ms	EPS ECU - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
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 ECU to turn on a warning light.	B	50 ms	EPS ECU - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
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.	B	50 ms	EPS ECU - Lane Departure Warning Safety Functionality	Lane departure torque is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	B	50 ms	EPS ECU – Data Transmission Integrity Check	N/A
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	EPS ECU – Memory Test	N/A

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-01 with its associated system elements

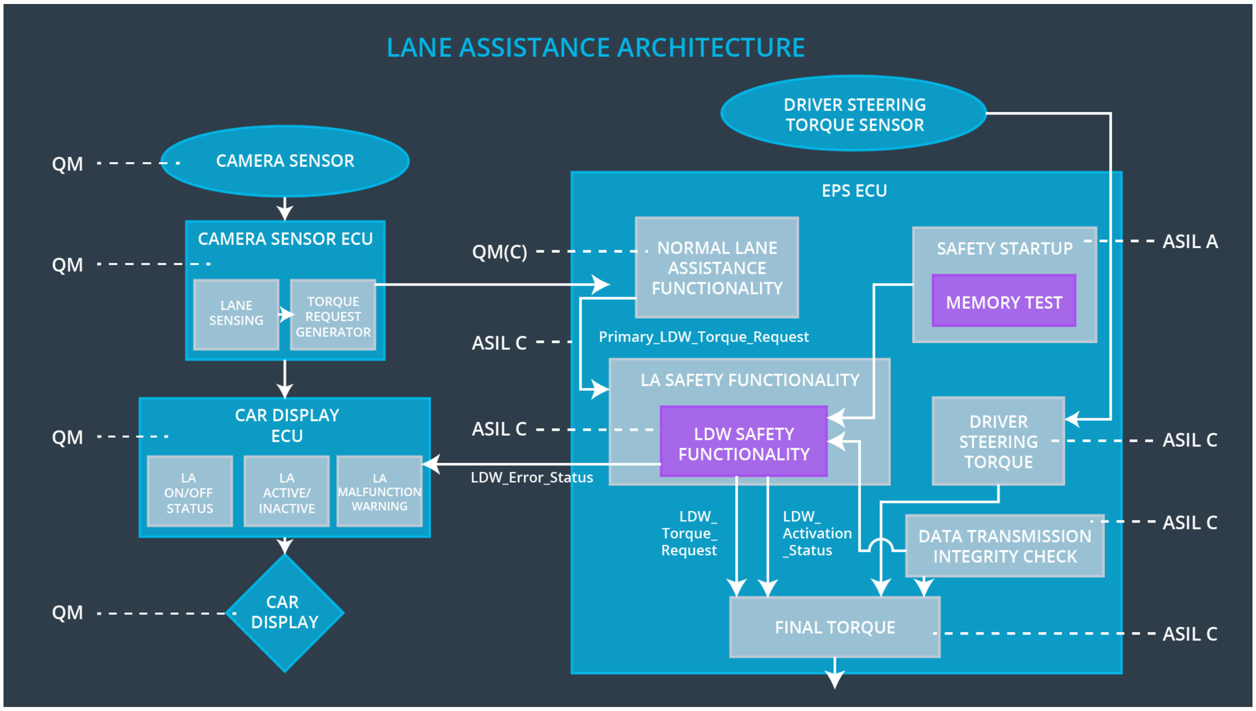
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety	The lane keeping item shall ensure that the lane keeping	X		

Requirement 02-01	assistance torque is applied for only Max_Duration			

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	LA safety component shall keep track of how long lane keeping functionality has been activated and ensure that the duration is less than Max_Duration.	B	500 ms	EPS ECU – Lane Keeping Assistance Safety Functionality	Lane keeping assistance function is deactivated.
Technical Safety Requirement 02	As soon as the LKA safety functionality deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to display a message the LKA is inactive.	B	500 ms	EPS ECU – Lane Keeping Assistance Safety Functionality	Lane keeping assistance function is deactivated.
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.	B	50 ms	EPS ECU – Lane Keeping Assistance Safety Functionality	Lane keeping assistance function is deactivated.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	EPS ECU – Data Transmission Integrity Check	N/A
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	EPS ECU – Memory Test	N/A

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the electronic power steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Driver Warning
WDC-01	Lane departure warning function turned off	Oscillating torque amplitude exceeds Max_Torque_Limit or oscillating torque frequency exceeds Max_Torque_Frequency or oscillating torque frequency drops below Min_Torque_Frequency	Car display shows message that lane departure warning is not available
WDC-02	Lane keep assistance	Lane keeping assistance torque is applied for	Car display shows message that lane keep

	function	greater than Max_Duration	assistance function is not available