Technical Safety Concept Lane Assistance

Document Version: [1]

Template Version 1.0, Released on 2017-09-15

Document history

Date	Version	Editor	Description
2017.09.16	1.0	Denise James	Initial Release
2017.09.28	2.0	Denise James	Add amplitude safety requirements
2017.10.11	3.0	Denise James	Change for Technical Safety Requirement 04 Architecture Allocation to "Data transmission integrity check"

Table of Contents

Purpose of the Technical Safety Concept

This technical functional safety requirements document takes the concept safety requirements and provides the detailed technical development requirements.

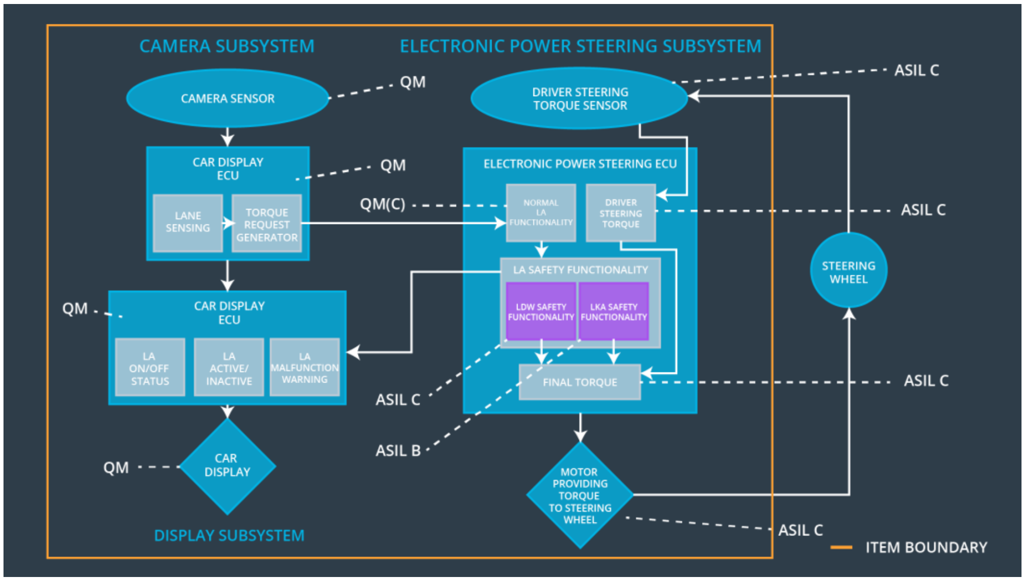
Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below $Max\_Torque\_Amplitude_2$	C	50 ms	LDW function is turned off with a lighted icon on the car display
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque frequency is below $Max\_Torque\_Frequency_2$	C	50 ms	LDW function is turned off with a lighted icon on the car display
Functional Safety Requirement 02-01	"The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration".	C	500 ms	LKA function is turned off with a lighted icon on the car display

Refined System Architecture from Functional Safety Concept

Figure 1 shows the refined system architecture from the functional safety document.



Functional overview of architecture elements

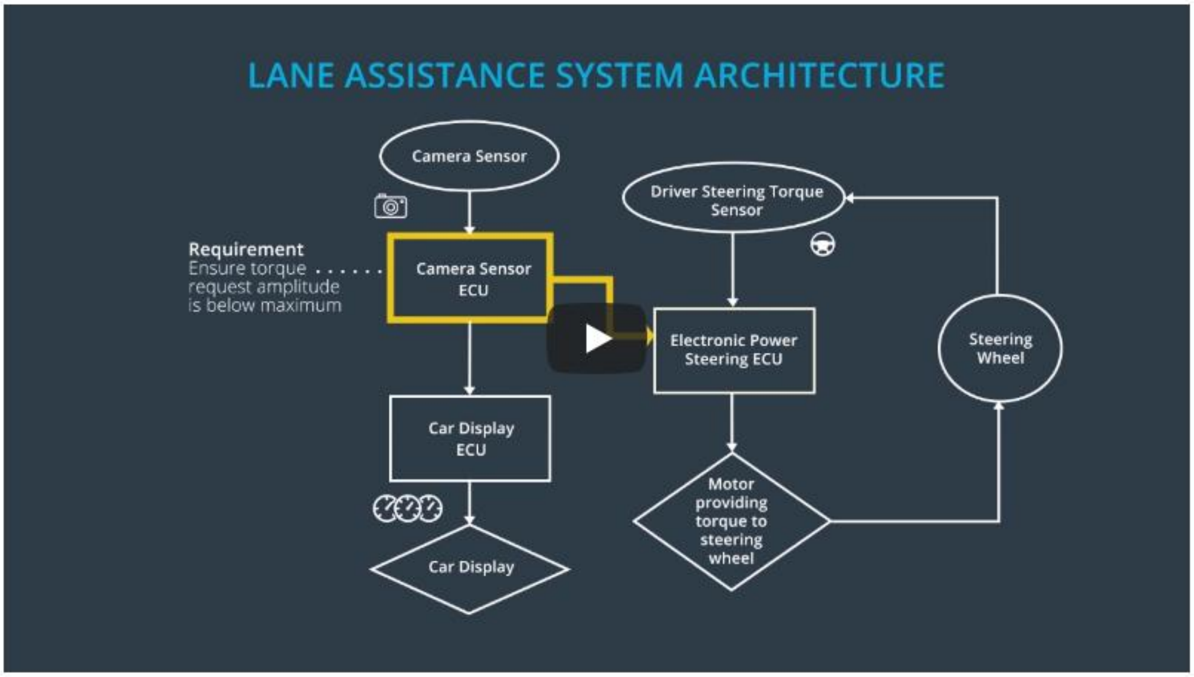
Element	Description
Camera Sensor	A sensor that detects analog information that represents an image. The sensor analog output is sent to the Car Display ECU
Camera (Car Sensor) Sensor ECU - Lane Sensing	The camera sensor analog output is sent to the Car Display ECU as an input. The car display ECU determines if a lane is in specifications. Status of the lane detection is displayed on the car display ECU.
Camera Sensor (Car Sensor) ECU - Torque request generator	A Torque Request is generated with inputs from the camera sensor information and the car display lane sensing information. These two inputs are used in the car display ECU to create the output, Torque Request to

	the Electronic Power Steering ECU.
Car Display	The car display shows the status of the following: 1. Lane Assist – ON/OFF 2. Lane Assist – Active/Inactive (if not ON as in #1, this is always Inactive) 3. Lane Assist – Malfunction (on if a malfunction in the LA function)
Car Display ECU - Lane Assistance On/Off Status	This function determines if the Lane Assist function is able to operate. The driver has control over turning this on or off. The car ECU display icon is an ISO 26262 standard. If this function is on, the icon is illuminated.
Car Display ECU - Lane Assistant Active/Inactive	If the Lane Assistance ON/OFF is on this Active/Inactive function may operate. If the car drives out of the lane it will oscillate the wheel for LDW and apply torque to move back to center for LKA function. The car ECU display icon for active/inactive is an ISO 26262 standard. If this function is on, the icon is illuminated.
Car Display ECU - Lane Assistance malfunction warning	If any of the safety goals are not met, this malfunction warning will activate. The car ECU display icon for malfunction is an ISO 26262 standard. If this function is on, the icon is illuminated
Driver Steering Torque Sensor	The sensor measures the steering rotational force applied by the driver and thus enables sensitive control of the electric steering support. The analog output of the Driver Steering Torque Sensor represents the torque applied by the driver. This output is sent to the Electronic Power Steering (EPS) ECU
Electronic Power Steering (EPS) ECU -	Electronic Power Steering (EPS) ECU takes an input from

Driver Steering Torque	the Driver Steering Torque Sensor. If the sensor is the normal operating range the EPS will send the final torque to the steering wheel. If the input torque sensor is over Max_Torque, a warning will be displayed on the ECU and safe torque value is sent to the steering wheel instead.
EPS ECU - Normal Lane Assistance Functionality	The Electronic Power Steering ECU sends the normal torque signal to the steering wheel.
EPS ECU - Lane Departure Warning Safety Functionality	The Electronic Power Steering ECU assures that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency and below Max_Torque_Amplitude
EPS ECU - Lane Keeping Assistant Safety Functionality	The Electronic Power Steering ECU assures that the duration of the applied torque is limited for safety requirements.
EPS ECU - Final Torque	If the driver steering torque sensor is the normal operating range the EPS will send the final torque to the steering wheel. If the input torque sensor is over Max_Torque, a warning will be displayed on the ECU and safe torque value is sent to the steering wheel instead.
Motor	The motor provides output torque to the steering wheel based on the EPS-ECU final torque input.

Technical Safety Requirements

Allocation of Requirements to the System Architecture


LANE ASSISTANCE SYSTEM ARCHITECTURE
Camera Sensor
Requirement
Ensure torque request amplitude is below maximum
Camera Sensor ECU
Driver Steering Torque Sensor
Electronic Power Steering ECU
Steering Wheel
Car Display ECU
Car Display
Motor providing torque to steering wheel

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 from the Functional Safety Document

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

Requirement 01-01	Max_Torque_Amplitude			

Five 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	Electronic Power Steering ECU (includes the LDW safety block)	LDW function turned off. Malfunction light on car display.
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	Data Transmission Integrity Check	LDW function turned off. Malfunction light on car display.
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	Electronic Power Steering ECU (includes the LDW safety block)	LDW function turned off. Malfunction light on car display.
Technical	As soon as the LDW function deactivates the LDW feature,	C	50 ms	Electronic Power Steering	LDW torque output is set to

Safety Requirement 04	the LDW Safety software block shall send a signal to the car display ECU to turn on a warning light			ECU (includes the LDW safety block)	zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	50 ms	Ignition Cycle	LDW torque output is set to zero

Functional Safety Requirement 01-02 from the Functional Safety Document

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		

Five 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	The LDW safety component shall ensure that the frequency of the	C	50 ms	Electronic Power Steering	LDW function

Safety Requirement 01	'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.			ECU (includes the LDW safety block)	turned off. Malfunction light on car display.
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	Data Transmission Integrity Check	LDW function turned off. Malfunction light on car display.
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	Electronic Power Steering ECU (includes the LDW safety block)	LDW function turned off. Malfunction light on car display.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Electronic Power Steering ECU(includes the LDW safety block)	LDW function turned off. Malfunction light on car display.
Technical Safety	Memory test shall be conducted at start up of the EPS ECU to check for	A	Ignition Cycle	Ignition cycle	LDW function turned

Requirement 05	any faults in memory.				off. Malfunction light on car display.

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 01-02 from the Functional Safety Document

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		

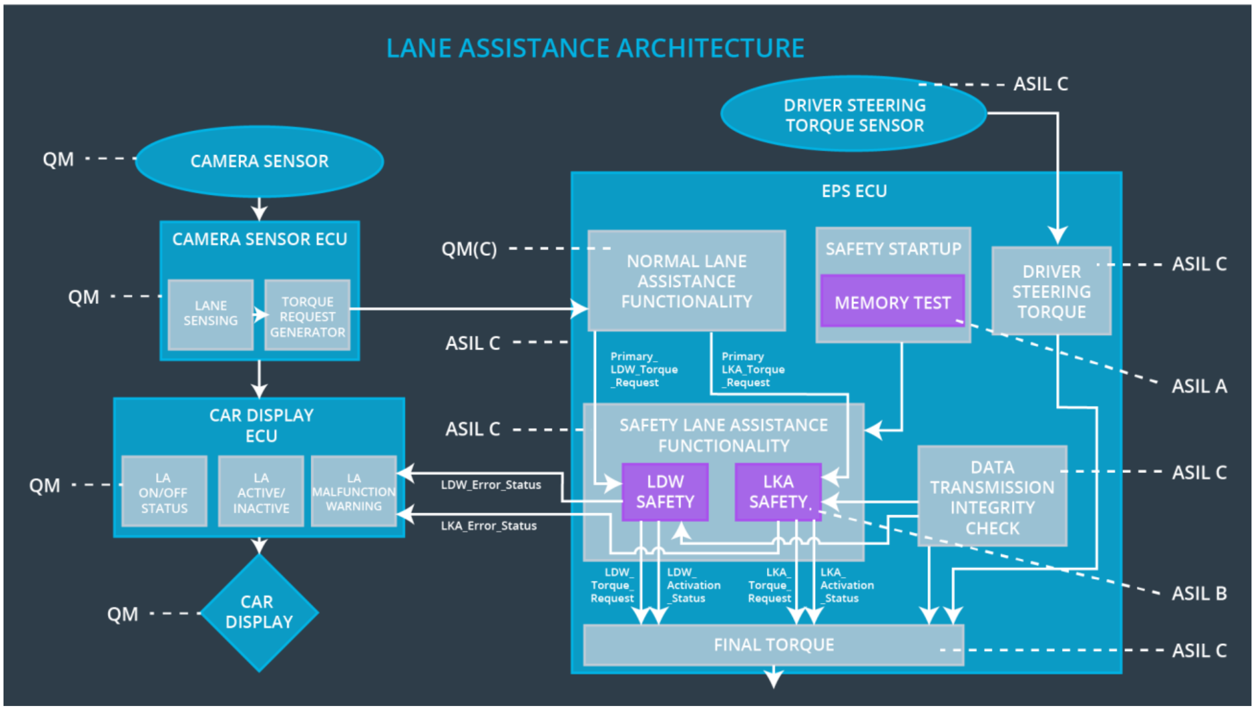
Five Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Electronic Power Steering ECU (includes the LKA safety block)	LKA function turned off. Malfunction light on car display.
Technical	As soon as the LKA function	B	500 ms	Electronic Power	LKA function turned off.

Safety Requirement 02	deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.			Steering ECU (includes the LKA safety block)	Malfunction light on car display.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LDW feature and the 'LKA_Torque_Request' shall be set to zero.	B	500 ms	Electronic Power Steering ECU (includes the LKA safety block)	LKA function turned off. Malfunction light on car display.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	A	500 ms	Electronic Power Steering ECU (includes the LKA safety block)	LKA function turned off. Malfunction light on car display.
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	Electronic Power Steering ECU (includes the LKA safety block)	LDW function turned off. Malfunction light on car display.

Refinement of the System Architecture

Below is a diagram of the system architecture after the safety technical requirements are applied.



Allocation of Technical Safety Requirements to Architecture Element

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	LDW function is turned off with a lighted icon on the car display	Max_Torque_Amplitude or Max_Torque_Freq is higher	YES	Icon lighted on car display.
WDC-02	LKA function is turned off with a lighted icon on the car display	lane keeping assistance torque is applied for longer than Max_Duration	YES	Icon lighted on car display.