Technical Safety Concept Lane Assistance

Document Version: 1.0

Released on 2018-06-21

Document history

Date	Version	Editor	Description
21-Jun-2018	1.0	Prathmesh Dali	Final Submission

Table of Contents

Purpose of the Technical Safety Concept

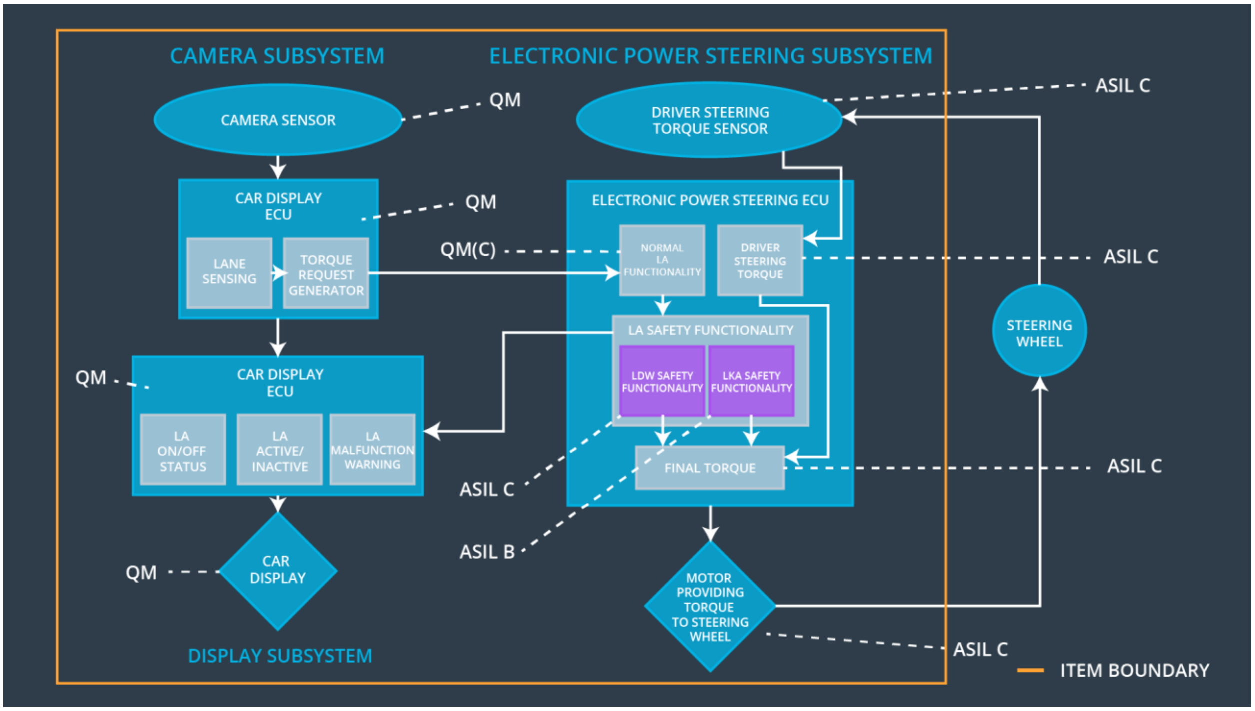
Its purpose is to specify the roadmap for implementation of the defined functional safety concept. This includes concrete information on item's technology.

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 less than Max_Torque_Amplitude value.	C	50 ms	Turn Off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is less than Max_Torque_Frequency value.	C	50 ms	Turn Off LDW
Functional Safety Requirement 02-01	Ensure that LKA torque is applied only for a limited time not more than Max_Duration	B	500 ms	Turn off LKA setting torque to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Sensors to capture environmental information as images and provide them to the camera sensor ECU continuously.
Camera Sensor ECU - Lane Sensing	A processor unit to process acquired images by camera sensors to detect Lane Lines and calculate car positions w.r.t. to lane lines.
Camera Sensor ECU - Torque request generator	A processor unit to generate Torque request to the car for the Electronic Power Steering ECU
Car Display	Display device to display system status and warnings during system malfunctions to driver.

Car Display ECU - Lane Assistance On/Off Status	A control function to display on/off status of lane assistance system.
Car Display ECU - Lane Assistant Active/Inactive	A control function to display active or inactive status of lane assistance system.
Car Display ECU - Lane Assistance malfunction warning	Function for displaying any malfunction in the Lane Assistance system
Driver Steering Torque Sensor	Sensor for measuring the torque applied to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Processing unit for processing input from driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	A function to process the data from the torque request generator
EPS ECU - Lane Departure Warning Safety Functionality	Checks for any malfunction in the LDW function and take appropriate action accordingly. (deactivate if there is any malfunction, pass the output torque to the final torque is there isn’t any malfunction)
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks for any malfunction in LKA function and take appropriate action. (deactivate if there is any malfunction, pass the output torque to the final torque is there isn’t any malfunction)
EPS ECU - Final Torque	Combine the inputs from LDW and LKA and deliver the final torque request to the motor
Motor	An electric motor that interpret the EPS ECU data to control 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	As soon as the failure is detected by the Lane Departure Warning function , it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero	C	50 ms	Lane Departure Warning Safety block	LDW Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 02	As soon as the Lane Departure Warning function deactivates the LDW feature , ‘LDW safety’ software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	Lane Departure Warning Safety block	LDW Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 03	Memory test should be conducted at startup of the EPS ECU to check for any FAULTS in memory	A	Ignition cycle	Data Transmission Integrity Check	LDW Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured.	C	50 ms	Lane Departure Warning Safety block	LDW Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 05	The Lane Departure Warning safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to	C	50 ms	Lane Departure Warning Safety block	LDW Torque Request Amplitude shall be set to zero.

	the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude.				

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	Once the failure is detected by the Lane Departure Warning function , it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall be set to zero	C	50 ms	Lane Departure Warning Safety Block	LDW Torque Request Frequency shall be set to zero.
Technical Safety Requirement 02	Once the Lane Departure Warning function deactivates the LDW feature , ‘LDW safety’ software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	Lane Departure Warning Safety Block	LDW Torque Request Frequency shall be set to zero

Technical Safety Requirement 03	Memory test should be conducted at startup of the EPS ECU to check for any FAULTS in memory	A	Ignition cycle	Data Transmission Integrity Check	LDW Torque Request Frequency shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request signal should be ensured.	C	50 ms	Lane Departure Warning Safety Block	LDW Torque Request Frequency shall be set to zero
Technical Safety Requirement 05	The Lane Departure Warning 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_Frequency	C	50 ms	Lane Departure Warning Safety Block	LDW Torque Request Frequency shall be set to zero

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

Lane Keeping Assistance (LKA) Requirements:

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

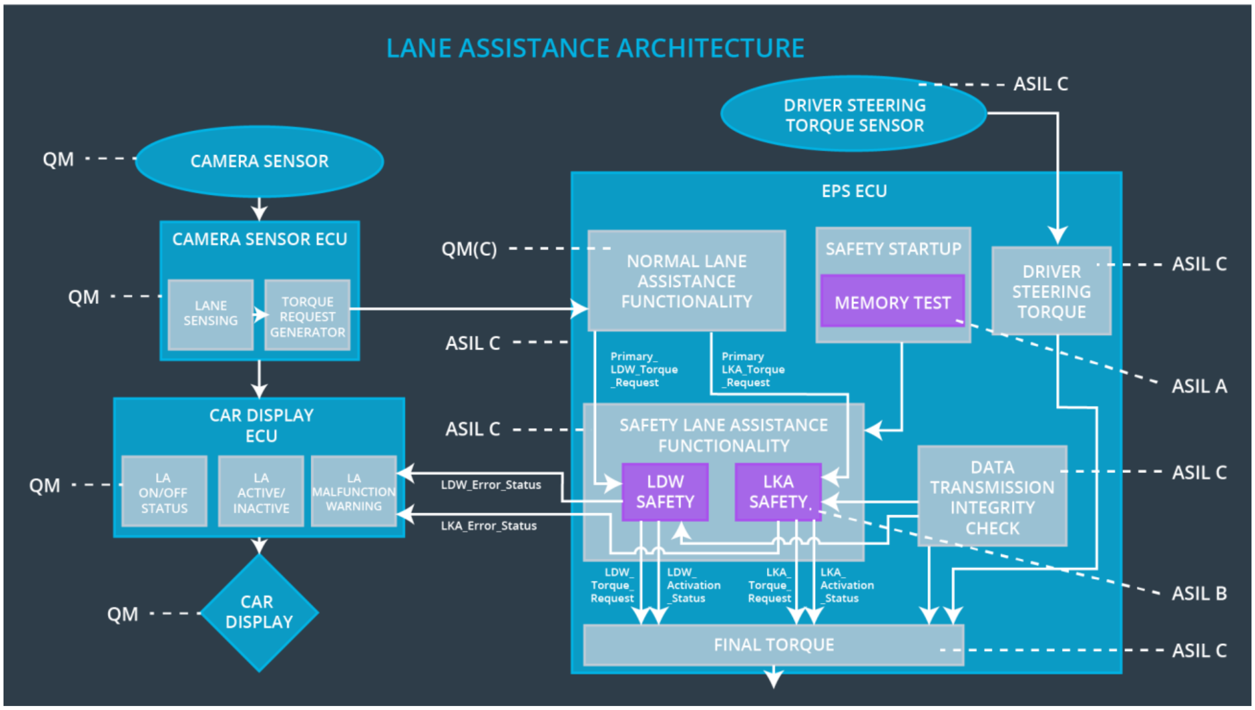
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 Lane Keeping Assistance safety component should ensure that the Duration of LKA Torque application is less than Max_Duration.	B	500 ms	Lane Keeping Assistance safety block	LKA Torque Request shall be set to zero
Technical Safety Requirement 02	Once the Lane Departure Warning 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	500 ms	Lane Keeping Assistance safety block	LKA Torque Request shall be set to zero
Technical Safety Requirement 03	Memory test should be conducted at startup of the EPS ECU to check for any FAULTS in memory	A	ignition cycle	Data Transmission Integrity Check	LKA Torque Request shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request signal should be ensured.	B	500 ms	Lane Keeping Assistance safety block	LKA Torque Request shall be set to zero
Technical Safety Requirement 05	The LKA safety component shall ensure that duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	B	500 ms	Lane Keeping Assistance safety block	LKA Torque Request shall be set to zero

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

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	Turn on warning light of the LDW functionality
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_04	Yes	Turn on warning light of the LKA functionality