Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
08.14.2018	1.0	Liang Zhang	First attempt

Table of Contents

Purpose of the Technical Safety Concept

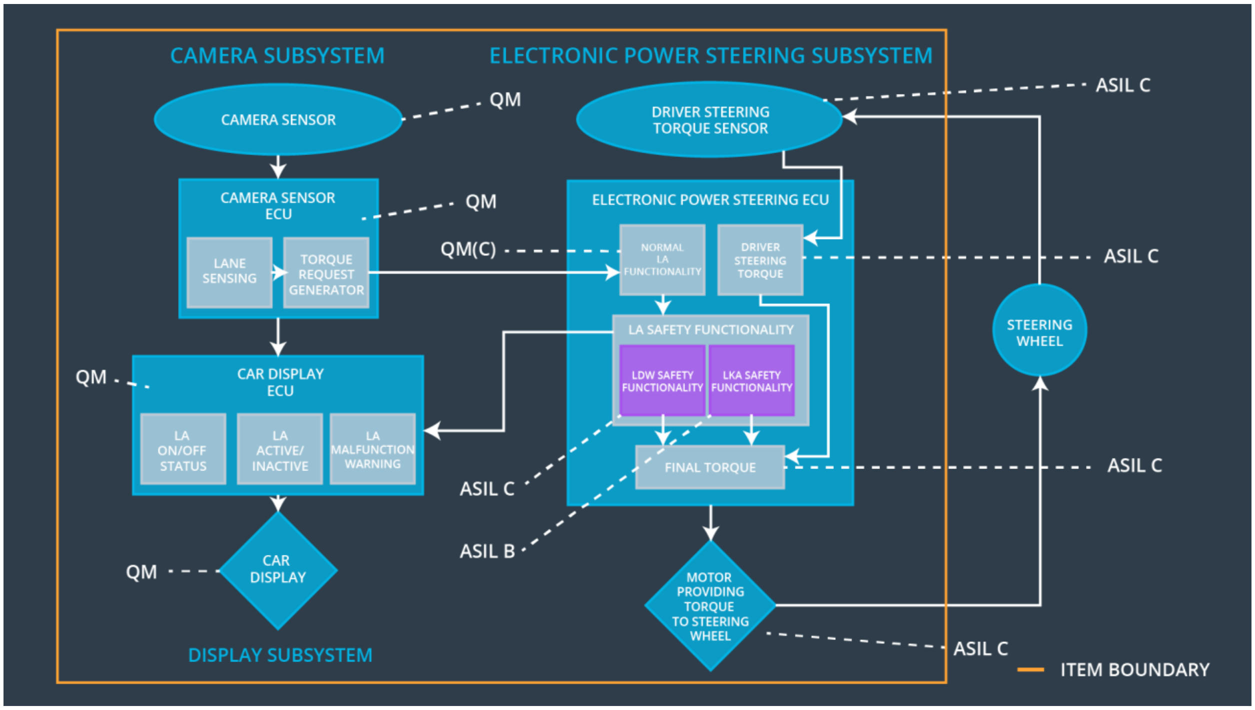
Derive more concrete requirements based on the safety requirements from functional safety concept. Allocate these requirements to elements of the item. Look at how the subsystems interact with each other and how elements inside of one ECU interact with each other.

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 oscillating torque is below Maximum_Torque_Amplitude.	C	50 ms	Turn off LDW component by setting oscillating_torque to zero
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque is below Maximum_Torque_Frequency.	C	50 ms	Turn off LDW component by setting oscillating_torque to zero
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	Turn off LKA component by setting steering_torque to zero.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Send recording images to camera sensor ECU.
Camera Sensor ECU - Lane Sensing	Extract lane boundary from images and identify if the vehicle departs from lane. If yes, send a message to Torque request generator.
Camera Sensor ECU - Torque request generator	Generate a torque request and send it to electronic power steering ECU.
Car Display	Inform driver the status of the lane assistance system and activation/deactivation of the system. Warn drivers if there is a malfunction.
Car Display ECU - Lane Assistance On/Off Status	Determine the status of Lane Assistance, then send the status to car display.
Car Display ECU - Lane Assistant Active/Inactive	Determine if Lane Assistance active or not, then send a signal to car display.
Car Display ECU - Lane Assistance malfunction warning	Determine if a malfunction occurs in the Lane Assistance system. If yes, send a warning signal to car display.

Driver Steering Torque Sensor	Measure amplitude, frequency and duration of oscillating/steering torque from steering wheel and send them to electronic power steering ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receive measurement from Driver Steering Torque Sensor, send a message to Final Torque component.
EPS ECU - Normal Lane Assistance Functionality	Process Torque request from Camera Sensor ECU, then send a message to LDW or LKA component.
EPS ECU - Lane Departure Warning Safety Functionality	Calculate how much oscillating torque is required, then send torque request to Final Torque component
EPS ECU - Lane Keeping Assistant Safety Functionality	Calculate how much steering torque is required, then send torque request to Final Torque component
EPS ECU - Final Torque	Calculate how much oscillating/steering torque is required, then send torque request to Motor.
Motor	Receive torque request from Final Torque component, then provide torque to 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	The lane keeping item shall ensure that the lane departure	X		

01-01	oscillating torque amplitude is below Max_Torque_Amplitude			

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 block	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ shall be ensured.	C	50 ms	Data Transmission Integrity Check	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 03	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	LDW safety block	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 04	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	LDW safety block	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems。	A	ignition cycle	Data Transmission Integrity Check	Deactivate the LDW feature and 'LDW_Torque_Request'

					shall be set to 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	C	50 ms	LDW safety block	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' shall be ensured.	C	50 ms	Data Transmission Integrity Check	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero

Technical Safety Requirement 03	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	LDW safety block	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 04	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	LDW safety block	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems。	A	ignition cycle	Data Transmission Integrity Check	Deactivate the LDW feature and 'LDW_Torque_Request' shall be set to 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	The lane keeping item shall	X		

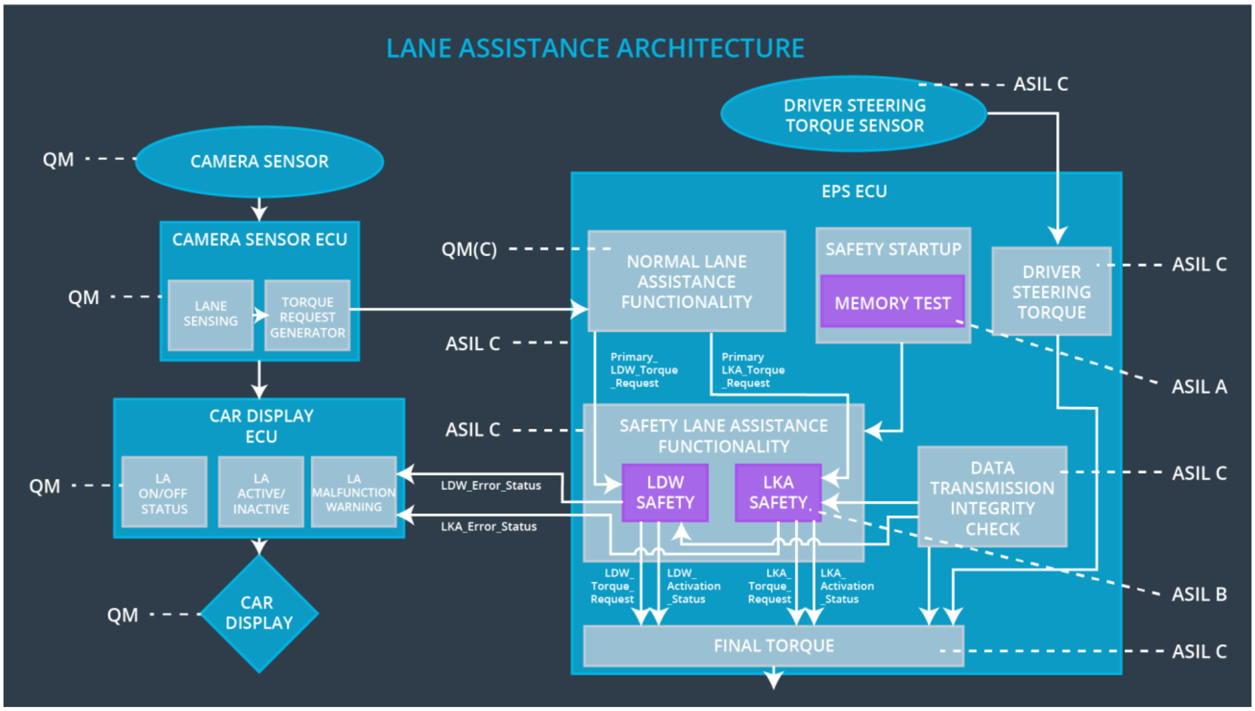
Safety Requirement 02-01	ensure that the lane keeping assistance torque is applied for only Max_Duration			

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	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 block	Deactivate the LKA feature and 'LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ shall be ensured.	B	500 ms	Data Transmission Integrity Check	Deactivate the LKA feature and 'LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 03	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LKA safety block	Deactivate the LKA feature and 'LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 04	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	500 ms	LKA safety block	Deactivate the LKA feature and 'LKA_Torque_Request' shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems。	A	ignition cycle	Data Transmission Integrity Check	Deactivate the LKA feature and 'LKA_Torque_Request' shall be set

					to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For 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	Turning the lane assistance system	The lane departure oscillating torque is above	Yes	A warning that the oscillating

	off, i.e. the torque request from the lane keeping assistance will be set to zero	Max_Torque_Amplitude or Max_Torque_Frequency		torque is above the maximum value
WDC-02	Turning the lane assistance system off, i.e. the torque request from the lane keeping assistance will be set to zero	The lane keeping assistance torque is applied longer than Max_Duration	Yes	A warning that this function is meant for autonomous driving