Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2019.07.28	1.0	Zhilong Lu	First Submission

Table of Contents

Contents

Document history 2

Table of Contents.. 3

Purpose of the Technical Safety Concept 4

Inputs to the Technical Safety Concept 4

Functional Safety Requirements 4

Refined System Architecture from Functional Safety Concept 4

Functional overview of architecture elements 5

Technical Safety Concept 6

Technical Safety Requirements 6

Refinement of the System Architecture...12

Allocation of Technical Safety Requirements to Architecture Elements 12

Warning and Degradation Concept...13

Purpose of the Technical Safety Concept

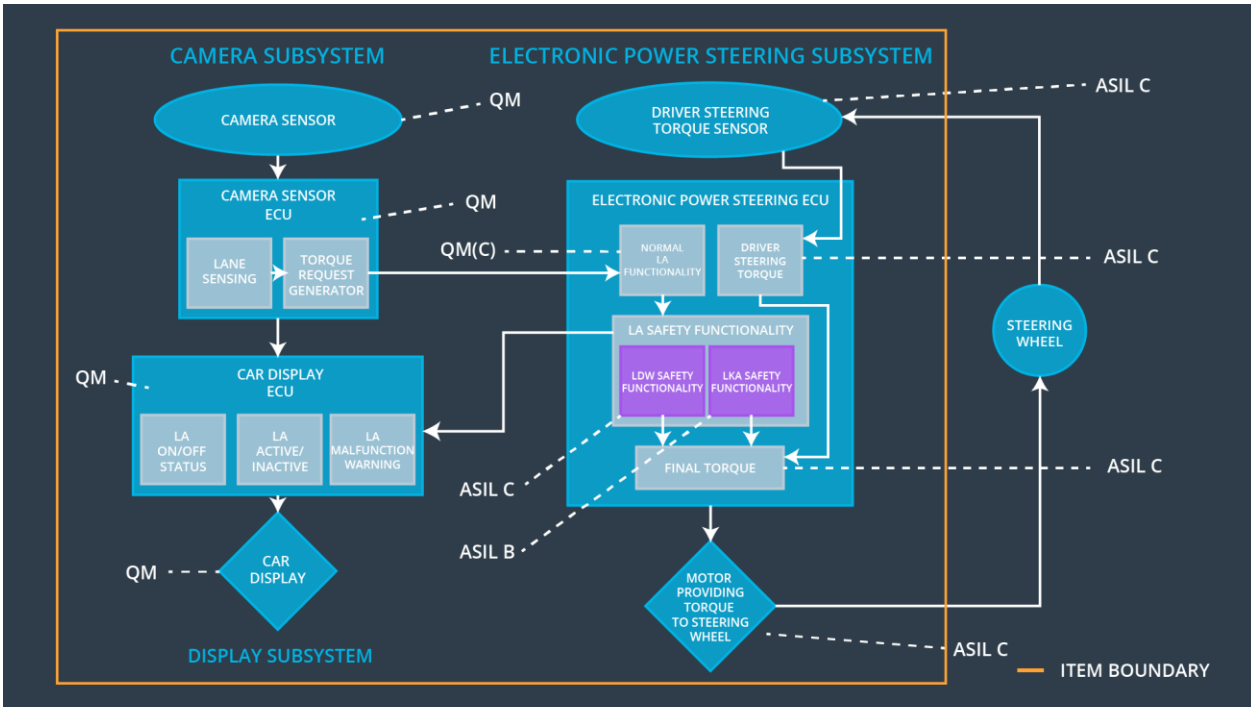
The Technical Safety Concept defines how the subsystems interact at the massage level and describes how the ECUs communicate with each other.

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 oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude.	C	50 ms	LDW will set the oscillating torque to 0.
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the oscillating torque frequency requested by the LDW function is below Max_Torque_Frequency.	C	50 ms	LDW will set the oscillating torque 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	LDW will set the oscillating torque to 0.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	The camera sensor reads in images from the road.
Camera Sensor ECU - Lane Sensing	The Lane Sensing element reads in an image from the Camera Sensor and extracts lane markings from that image.
Camera Sensor ECU - Torque request generator	The Torque request generator derives a steering torque based on the sensed lane markings and the current vehicle position and sends it to the Electronic Power Steering ECU.
Car Display	The Car Display shows a warning light to the driver, when the vehicle leaves the lane.
Car Display ECU - Lane Assistance On/Off Status	The Lane Assistance On/Off Status indicates whether the Lane Assistance System is turned on or off by the driver.
Car Display ECU - Lane Assistant Active/Inactive	The Lane Assistant Active/Inactive indicates whether the Lane Assistant System is fully

	operational (e.g. has found lane markings an is able to apply a steering torque).
Car Display ECU - Lane Assistance malfunction warning	The Lane Assistance malfunction warning indicates that the system is deviated, and it is shut down (or degraded).
Driver Steering Torque Sensor	The Driver Steering Torque Sensor provides the torque that the driver puts on the steering wheel to the Electronic Power Steering ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Driver Steering Element reads in the signal from the Driver Steering Torque Sensor which indicates how much (torque) the driver is steering.
EPS ECU - Normal Lane Assistance Functionality	The Normal Lane Assistance Functionality
EPS ECU - Lane Departure Warning Safety Functionality	This Element receives the torque demand from the Torque request generator in the Camera Sensor ECU and limits the vibration torque to the amplitude and frequency limit.
EPS ECU - Lane Keeping Assistant Safety Functionality	The Safety Functionality Element takes care of the functional safety requirements (e.g. it ensures the limits on the vibration torque and the maximum time on the Lane Keeping functionality.
EPS ECU - Final Torque	The Final Torque outputs a final torque based on the torque demand from the Normal Lane Assistance Functionality and the driver steering torque.
Motor	The Motor applies the demanded torque that is demanded by the Electronic Power Steering ECU onto 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	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	LDW shall set the oscillating torque 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	LDW Safety block	LDW shall set the oscillating torque 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	LDW Safety block	LDW shall set the oscillating torque 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	Data Transmission Integrity Check	LDW shall set the oscillating torque to 0.
Technical Safety Requirem	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Safety Startup Memory Test	LDW shall set the oscillating torque to 0.

ent 05					

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 block	LDW torque request amplitude shall be set to zero.
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	LDW Safety block	LDW torque request amplitude shall be set to zero.
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	LDW Safety block	LDW torque request amplitude shall be set to zero.
Technical Safety	The validity and integrity of the data transmission for	C	50 ms	Data Transmission	LDW torque

Requirement 04	‘LDW_Torque_Request’ signal shall be ensured.			Integrity Check	request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Memory Test	LDW torque request amplitude shall be set to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Make a study to test how drivers react to different torque amplitudes/frequencies to prove that we chose an appropriate value for ‘Max_Torque_Amplitude’/’Max_Torque_Frequency’.	Do a software test by inserting a fault into the system. When the demanded torque amplitude/frequency crosses the limit ‘Max_Torque_Amplitude’/’Max_Torque_Frequency’, the lane assistance output must be set to zeros within 50 ms.
Technical Safety Requirement 02	Make a study to test how drivers react on the warning light when the LDW function deactivates the LDW feature.	Do a software test with Electronic Power Steering ECU, Car Display ECU and its communication. When setting primary ‘LDW_Torque_Request’ outside the limits ‘Max_Torque_Amplitude’/’Max_Torque_Frequency’ the Car Display must show the warning light.
Technical Safety Requirement 03	Make a study to test how drivers react on the total loss of steering vibration torque when the LDW function deactivates the LDW feature.	Do a software test with the Electronic Power Steering ECU. When setting the primary ‘LDW_Torque_Request’ outside the limits ‘Max_Torque_Amplitude’/’Max_Torque_Frequency’, the signal ‘LDW_Torque_Request’ from the Safety Lane Assistance Functionality Block must be 0.
Technical Safety	- no validation possible -	Do a software test with the Electronic Power Steering ECU, Car Display ECU and

Requirement 04		its communication. The data that is transmitted from EPS ECU to Car Display ECU shall not be deviated. Artificial communication errors shall be detected.
Technical Safety Requirement 05	- no validation possible -	Do a software test with the EPS ECU by artificially altering the memory. The memory check shall find all memory deviations.

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 signal ‘LKA_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is only active for ‘Max_Duration’.	B	500 ms	LKA Safety block	LKA torque request amplitude shall be set to zero.
Technical Safety Requirement	As soon as the LKA function deactivates the LKA feature, the ‘LKA Safety’ software block shall send a signal to the car display	B	500 ms	LKA Safety block	LKA torque request amplitude shall be set

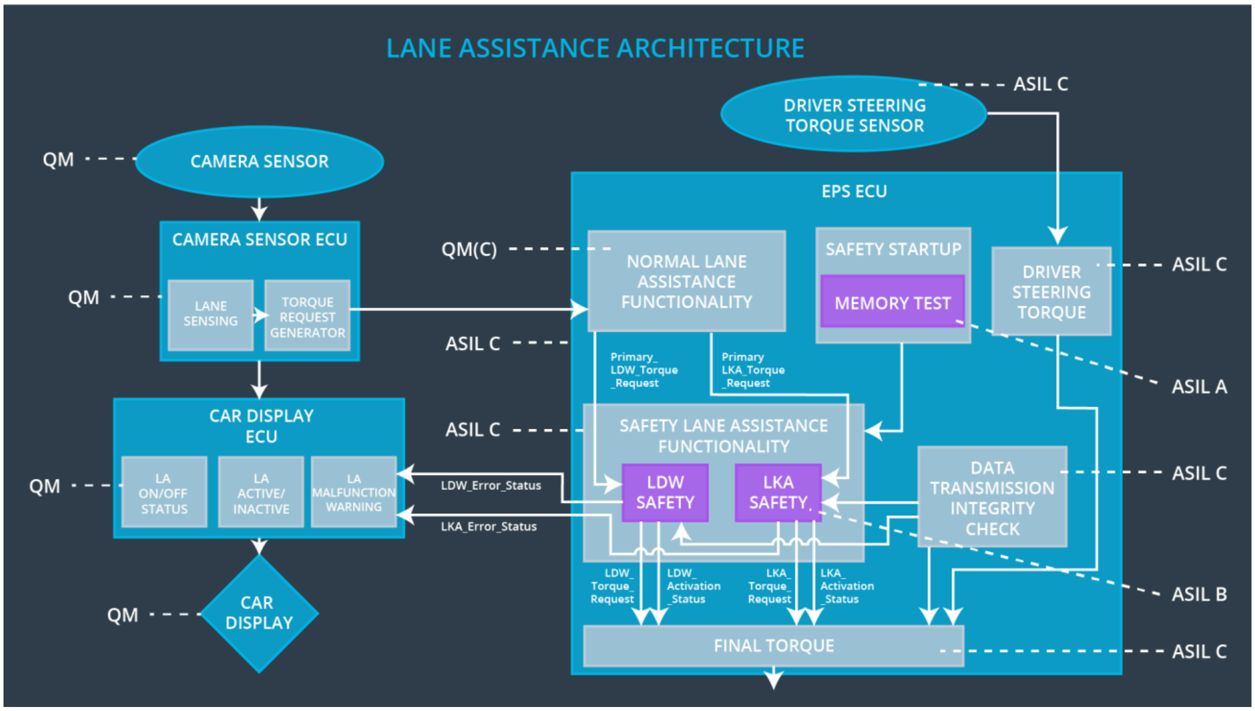
02	ECU to turn on a warning ligth.				to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ‘LKA_Torque_Request’ shall be set to zero.	B	500 ms	LKA Safety block	LKA torque request amplitude shall be set to zero.
Technical 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 torque request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Safety Startup Memory Test	LKA torque request amplitude shall be set to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Make a study to test that the time ‘Max_Duration’ chosen really dissuades drivers from taking their hands off the wheel.Make car or software tests that the system really does turn off if the lane keeping assistance ever exceeded max_duration.	Make car or software tests that the system really does turn off if the lane keeping assistance ever exceeded max_duration.
Technical Safety Requirement 02	Make a study to test how drivers react on the warning light when the LKA function deactivates the LKA feature.	Do a software test with Electronic Power Steering ECU, Car Display ECU and its communication. When the time ‘Max_Duration’ passes without a torque from the driver, the Car Display must show the warning light.
Technical Safety Requirement 03	Make a study to test how drivers react on the total loss of steering support torque when the LKA function deactivates the LKA	Do a software test with the Electronic Power Steering ECU. When the time ‘Max_Duration’ passes without a torque from the driver, the signal ‘LKA_Torque_Request’ from the Safety

	feature.	Lane Assistance Functionality Block must be 0.
Technical Safety Requirement 04	- no validation possible -	Do a software test with the Electronic Power Steering ECU, Car Display ECU and its communication. The data that is transmitted from EPS ECU to Car Display ECU shall not be deviated. Artificial communication errors shall be detected.
Technical Safety Requirement 05	- no validation possible -	Do a software test with the EPS ECU by artificially altering the memory. The memory check shall find all memory deviations.

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	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality – Set torque request to 0	The lane departure warning function applies an oscillating torque with very high torque amplitude or torque frequency (above limit).	Yes	A message on the car display shows the driver, that the lane departure warning function is not available.
WDC-02	Turn off the functionality – Set torque request to 0	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	Yes	A message on the car display shows the driver, that the lane keeping assistance function is not available.