Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
4/29/2018	1.0	Yury Astashonok	First revision

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the Technical Safety Concept is to derive technical safety requirement from functional safety requirements for the Lane Assistance item and allocate the requirements to the system architecture.

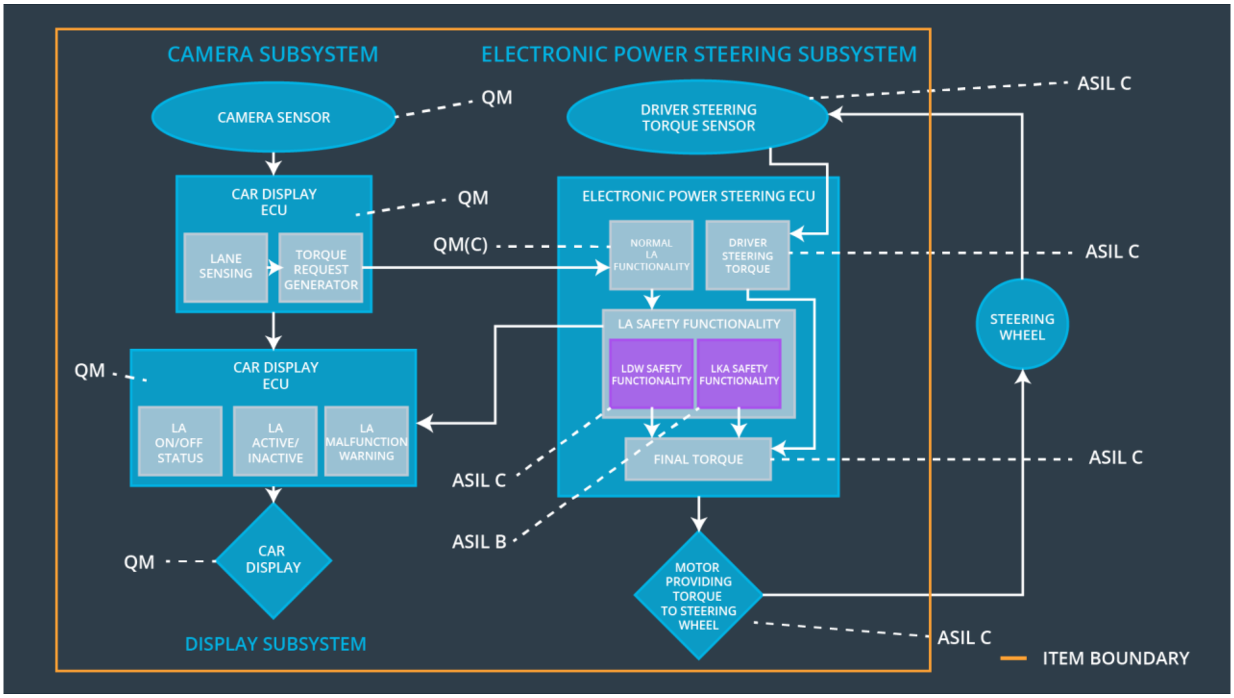
Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	A	Fault	Safe State

		SIL	**Tolerant Time Interval**	
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	The Lane Assistance functionality is switched off.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	The Lane Assistance functionality is switched off.
Functional Safety Requirement 01-03	The lane keeping item shall ensure that the lane departure oscillating torque frequency is above Min_Torque_Frequency.	B	50 ms	The Lane Assistance functionality is switched off.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied only when the function is activated.	C	50 ms	The Lane Assistance functionality is switched off.
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	The Lane Assistance functionality is switched off.

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 Camera Sensor ECU – Lane Sensing element identifies when the vehicle is leaving the lane.
Camera Sensor ECU – Torque request generator	The Camera Sensor ECU – Torque request generator sends signals to Electronic Power Steering ECU and Car Display ECU.
Car Display	The Car Display provides a visual feedback to the driver by turning on status lights.
Car Display ECU – Lane Assistance On/Off Status	The Car Display ECU – Lane Assistance On/Off Status element sends a signal to the Car Display to turn on the Lane Assistance On status light.
Car Display ECU – Lane Assistant Active/Inactive	The Car Display ECU – Lane Assistant Active/Inactive element sends a signal to the Car Display to turn on the Lane Assistance Active status light.
Car Display ECU – Lane Assistance malfunction warning	The Car Display ECU – Lane Assistance malfunction warning element sends a signal to the

	Car Display to turn on the Lane Assistance Malfunction warning light.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor detects the amount of torque applied by the driver to the steering wheel.
Electronic Power Steering (EPS) ECU – Driver Steering Torque	The Electronic Power Steering ECU – Driver Steering Torque element sends a signal from the Driver Steering Torque Sensor to the Final Torque element with the amount of torque applied by the driver.
EPS ECU – Normal Lane Assistance Functionality	The EPS ECU – Normal Lane Assistance Functionality element sends messages from Torque Request Generator to Lane Assistance Safety module.
EPS ECU – Lane Departure Warning Safety Functionality	The EPS ECU – Lane Departure Warning Safety Functionality element ensures that the LDW functionality does not malfunction.
EPS ECU – Lane Keeping Assistant Safety Functionality	EPS ECU – Lane Keeping Assistant Safety Functionality element ensures that the LKA functionality does not malfunction.
EPS ECU – Final Torque	The EPS ECU – Final Torque element combines signals from Lane Assistance Safety module and Driver Steering Torque module and sends a signal to the Motor.
Motor	The Motor provides a haptic feedback to the driver by adding extra torque to 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	LDW torque output 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	LDW Safety	LDW torque output 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	LDW Safety	LDW torque output 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	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	Memory Test	LDW torque output is set to 0.

Functional Safety Requirement 01-02 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	LDW torque output 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	LDW Safety	LDW torque output 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	LDW Safety	LDW torque output 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	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	Memory Test	LDW torque output is set to 0.

Functional Safety Requirement 01-03 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 01-03	The lane keeping item shall ensure that the lane departure oscillating torque frequency is above Min_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 above 'Min_Torque_Frequency.	C	50 ms	LDW Safety	LDW torque output 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	LDW Safety	LDW torque output 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	LDW Safety	LDW torque output 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	Data Transmission Integrity Check	N/A
Technical Safety Requirement	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW torque output

05					is set to 0.

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

LDW Validation Acceptance Criteria — perform a preliminary safety audit with a Safety Manager.

LDW Verification Acceptance Criteria — software tests should be implemented to verify the correct behavior of each technical safety requirement.

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 electronic power steering ECU shall ensure that the lane keeping assistance torque is applied only when the function is activated.	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 amplitude of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is above zero only when 'LKA_Activation_Status' signal is active.	B	50 ms	LKA Safety	LKA torque output is set to 0.
Technical Safety	As soon as the LKA function deactivates the LKA feature, the	B	50 ms	LKA Safety	LKA torque output is set

Requirement 02	'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.				to 0.
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	LKA Safety	LKA torque output is set to 0.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	50 ms	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	Memory Test	LKA torque output is set to 0.

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 02-02	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 02-02 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'	B	500 ms	LKA Safety	LKA torque output is set to 0.

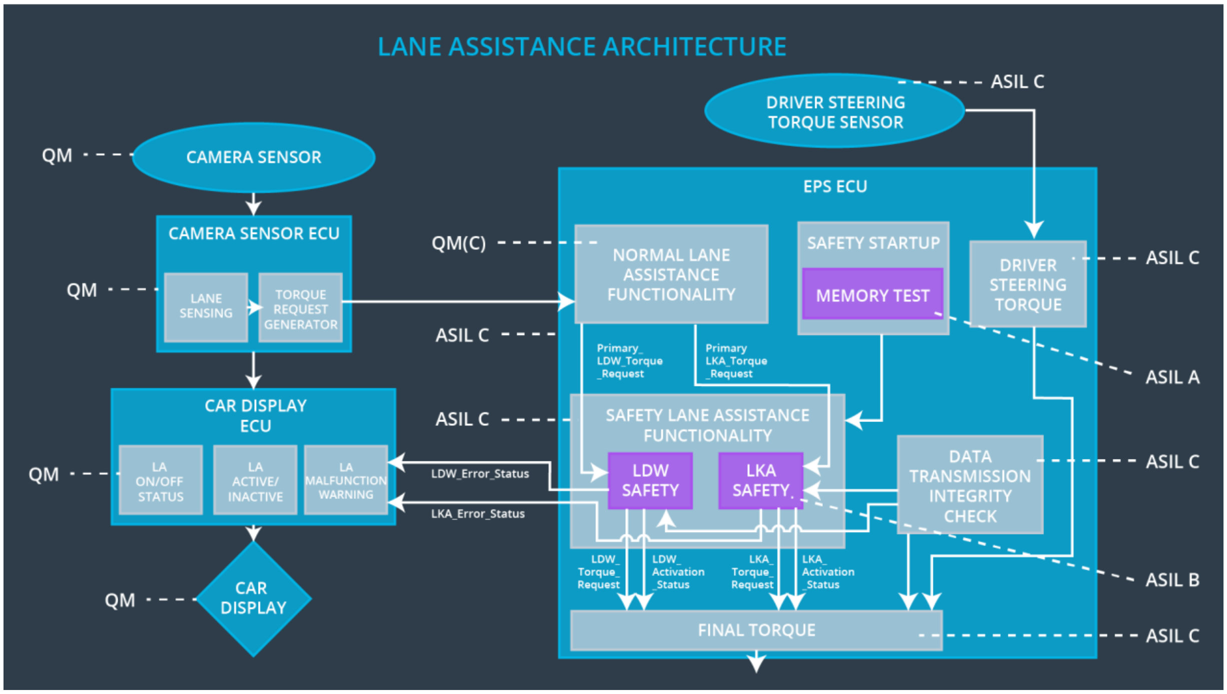
	component is no longer than 'Max_Duration'.				
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LKA Safety	LKA torque output is set to 0.
Technical 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	LKA torque output is set to 0.
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	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	Memory Test	LKA torque output is set to 0.

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

LKA Validation Acceptance Criteria — perform a preliminary safety audit with a Safety Manager.

LKA Verification Acceptance Criteria — software tests should be implemented to verify the correct behavior of each technical safety requirement.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements for the Lane Assistance item are allocated to the Electronic Power Steering ECU. Reference Functional Safety Concept for details.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality	LDW applies oscillating torque with amplitude above Max_Torque_Amplitude	Yes	Turn on a warning light on the dashboard
WDC-02	Turn off the functionality	LDW applies oscillating torque with frequency above Max_Torque_Frequency	Yes	Turn on a warning light on the dashboard
WDC-03	Turn off the functionality	LDW applies oscillating torque with frequency below Min_Torque_Frequency	Yes	Turn on a warning light on the dashboard
WDC-04	Turn off the functionality	LKA applies torque when not activated	Yes	Turn on a warning light on the dashboard
WDC-05	Turn off the	LKA applies torque longer than	Yes	Turn on a warning

	functionality	Max_Duration		light on the dashboard