Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [1]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
10/10/2017	0.1	Gustavo Espindola	First draft
11/10/2017	1	Gustavo Espindola	Release Candidate
18/10/2017	1.1	Gustavo Espindola	Minor corrections from reviewer

Table of Contents

Inhalt

Purpose of the Technical Safety Concept

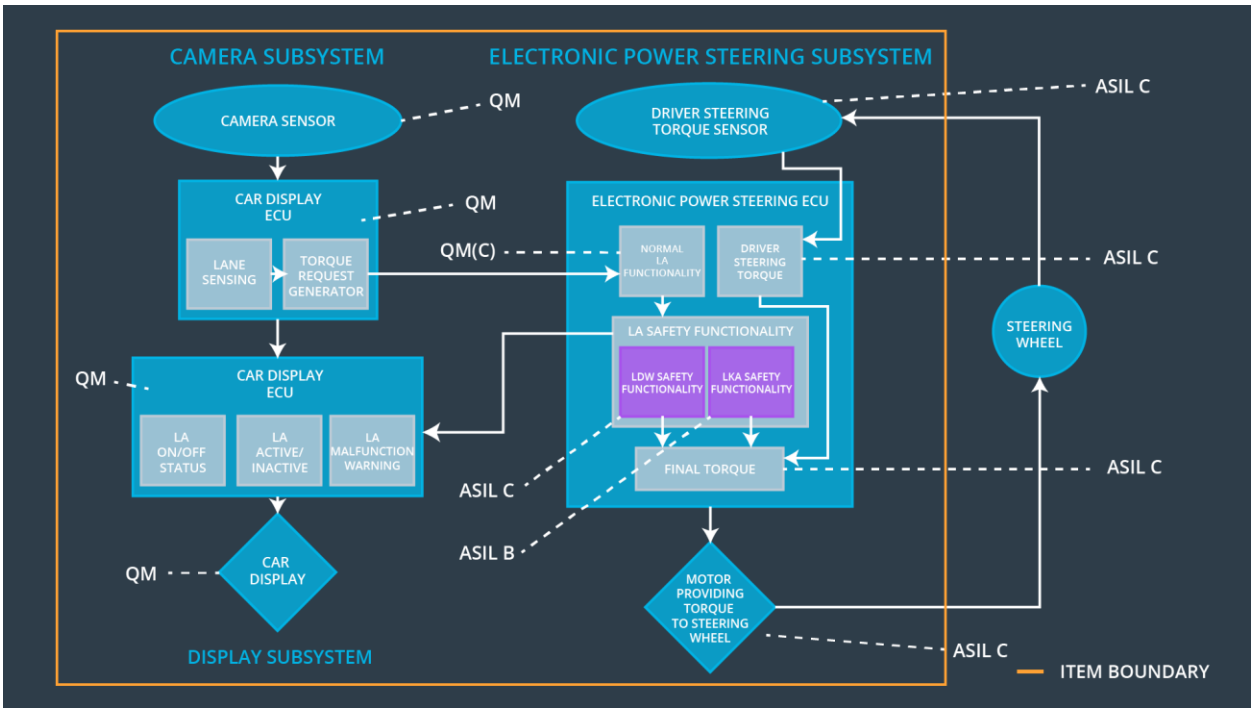
This document derives the functional safety requirements from the safety goals, and allocates them to an architectural element. This will delineate the hardware and software architecture as well as the safety mechanisms to be implemented.

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 limit the alert for the LDW, so the amplitude of the oscillating torque is less than Max_Torque_Amplitude	C	50ms	LDW requested torque is set to zero. The failure is shown in the car display and recorded.
Functional Safety Requirement 01-02	The electronic power steering ECU shall limit the alert for the LDW, so the frequency of the oscillating torque is less than Max_Torque_Frequency	C	50ms	LDW requested torque is set to zero. The failure is shown in the car display and recorded.
Functional Safety Requirement 02-01	The power steering ECU shall limit the duration of the functionality up to a period of Max_Duration	B	500ms	LKA requested torque is zero.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Obtains the image as raw data.
Camera Sensor ECU - Lane Sensing	Extract the lane lines and calculates the if the vehicle is inside the lane.
Camera Sensor ECU - Torque request generator	With the information of the Lane Sensing ECU, calculates the torque needed to keep the lane and correct the deviation. Then communicates with the electronic power steering ECU.

Car Display	Shows information about the state of the system: • System active/inactive • Lane assist on-line/off-line • Lane assist malfunction
Car Display ECU - Lane Assistance On/Off Status	Indicates that the Lane Assistance is not enabled.
Car Display ECU - Lane Assistant Active/Inactive	Indicates whether the system is correcting the direction of the vehicle or is just passive at the moment but ready.
Car Display ECU - Lane Assistance malfunction warning	If this lamp is active the lane assistance system was found faulty by itself or by another unit.
Driver Steering Torque Sensor	This sensor gives feedback on the force applied to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes the messages from the torque sensor and sends the required torque to achieve the requested torque if it is within the limits.
EPS ECU - Normal Lane Assistance Functionality	Processes the nominal signals from the camera subsystem which are not safety relevant.
EPS ECU - Lane Departure Warning Safety Functionality	Imposes the limits in frequency and amplitude to the received signal.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures the limited span of time in the functionality of the LKA system.
EPS ECU - Final Torque	This functionality is the responsible of monitor and ensure the correctness of the requested torque. If the requested torque is out of limits a failure is set.
Motor	Provides the physical result in the system, which is the torque being applied in the steering column.

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	50ms	Power Steering ECU – here the LDW safety block shall be implemented.	LDW functionality set off and requested torque 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	50ms	Power Steering ECU – here the LDW safety block shall be implemented.	LDW functionality set off and requested torque 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	50ms	Power Steering ECU – here the LDW safety block shall be implemented.	LDW functionality set off and requested torque set to 0.
Technical Safety Requirement 04	The validity and integrity of the safety data signal ‘LDW_Torque_Request‘ shall be ensured.	C	50ms after faulty message	Power Steering ECU – Data transmission integrity check	LDW functionality set off and requested torque set to 0. (Unknowns

					state of the system)
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Duration of ignition cycle	Safety startup - Memory test	LDW functionality set off and requested torque set to 0.

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 frequencies of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50ms	Power Steering ECU -- here the LDW safety block shall be implemented	LDW functionality set off and requested torque 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	50ms	Power Steering ECU. -- here the LDW safety block shall be	LDW functionality set off and request

				implemented	ed torque 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	50ms	Power Steering ECU. -- here the LDW safety block shall be implemented	LDW function ality set off and request ed torque set to 0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Power Steering ECU – Data transmission integrity check	LDW function ality set off and request ed torque set to 0. (Unkno wns state of the system)
Technical Safety Requirement 05	Memory test shall be conducted at start-up of the EPS ECU to check for any faults in memory	A	Duration of the ignition cycle	Power Steering ECU - Safety startup - Memory test	LDW function ality set off and request ed torque set to 0. (Unkno wns state of the system)

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		

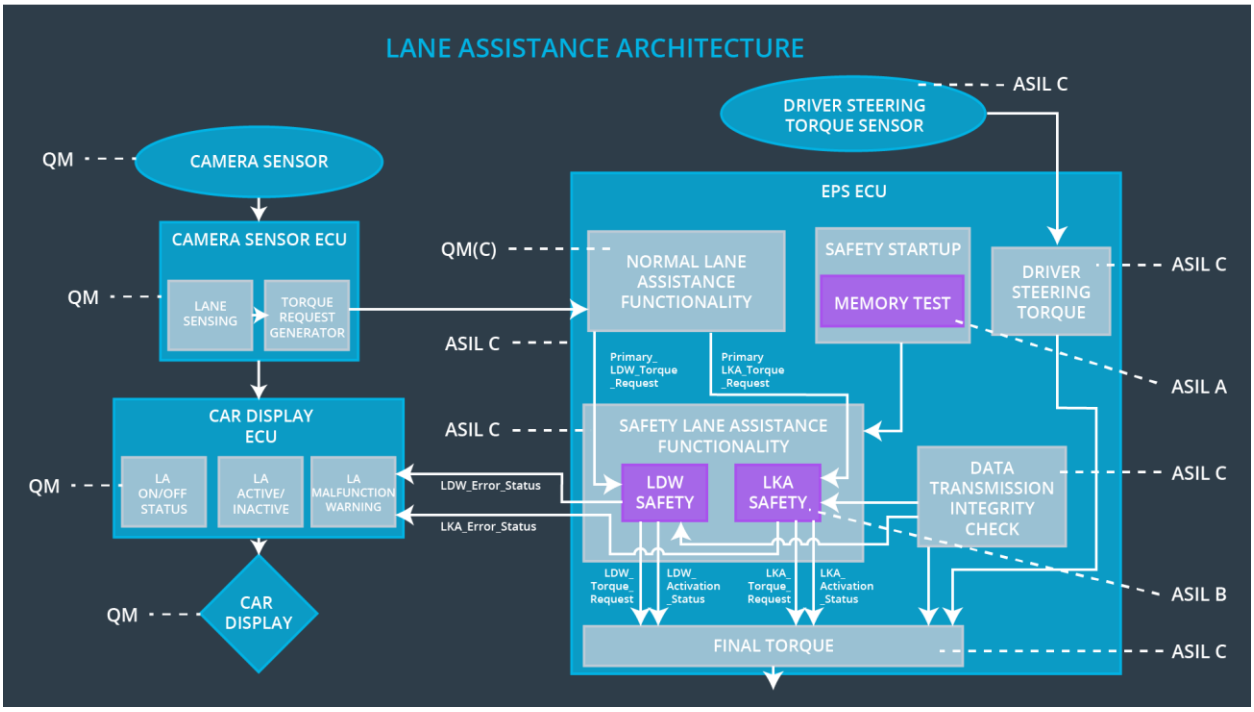
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The safety block for the LKA shall ensure that the functionality is active for a Max_Duration at most.	B	500 ms	Power Steering ECU – The safety LKA block	LKA functionality set off and requested torque set to 0.
Technical Safety Requirement 02	As soon as a failure in the LKA is detected, the functionality shall be deactivated, then the safety block shall send a signal to the display ECU to turn-on the failure lamp.	B	500ms	Power Steering ECU – The safety LKA block	LKA functionality set off and requested torque 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	500ms	Power Steering ECU – The safety LKA block	LKA functionality set off and requested torque set to 0.
Technical	The validity and integrity of the	B	500ms	Power Steering	LKA

Safety Requirement 04	data transmission for 'LKA_Torque_Request' signal shall be ensured.			ECU – The safety LKA block	functionality set off and requested torque set to 0. (Unknowns state of the system)
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Duration of the ignition cycle	ECU bootloader	LKA functionality set off and requested torque set to 0. Software is not reliable.

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	LDW functionality is deactivated and lamp turned on.	Requested oscillation amplitude is > Max_Torque_Amplitude OR Requested oscillation frequency is > Max_Torque_Frequency	Yes	Yes, through lamp in the dash board.
WDC-02	LKA functionality is deactivated and lamp turned on.	LKA functionality is active after Max_Duration	Yes	Yes, through lamp in the dash board.