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
28.10.2017	1.0	Simon Ritzel	First Draft and Submission

Table of Contents

Purpose of the Technical Safety Concept

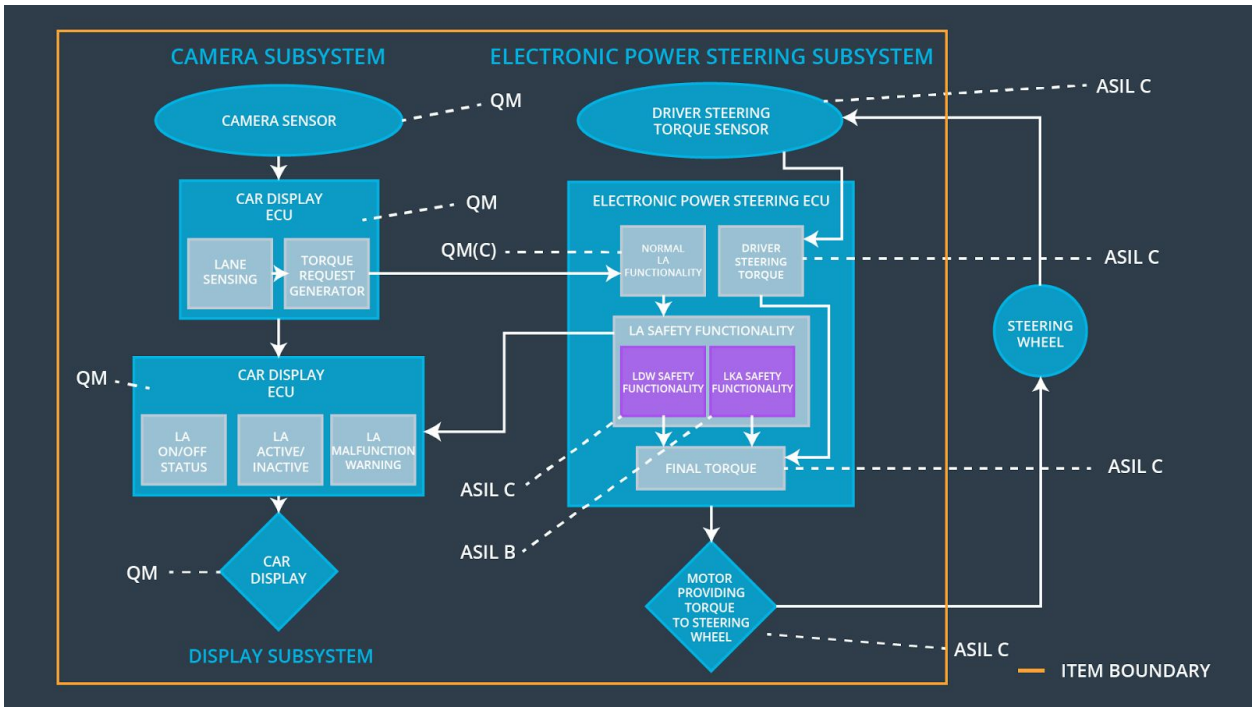
The goal of the Technical Safety Concept is to refine the functional safety requirements from the Functional Safety Concept into technical safety requirements.

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 *amplitude* is below Max_Torque_Amplitude	C	50 ms	LDW function is turned off with visual signal to the driver on the car display
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque *frequency* is below Max_Torque_Frequency	C	50 ms	LDW function is turned off with visual signal to the driver on the car display
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane assistance torque is applied for a maximum of Max_Duration	B	500 ms	LKA is turned off with visual signal on the car display to the driver.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures the images
Camera Sensor ECU - Lane Sensing	Extracts the lane lines from raw images and calculates the distance to the center of tha lane
Camera Sensor ECU - Torque request generator	Calculates the torque to steer the vehicle back to center of lane
Car Display	Displays state of the system
Car Display ECU - Lane Assistance On/Off Status	Shows if Lane Assistance is enabled
Car Display ECU - Lane Assistant Active/Inactive	Shows if Lane Assistant is actively steering the vehicle
Car Display ECU - Lane Assistance malfunction warning	Shows if the Lane Assistance works properly
Driver Steering Torque Sensor	Measures the torque from driver at the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads the measurements from the Driver Steering Torque Sensor
EPS ECU - Normal Lane Assistance Functionality	Processes nominal signals from the Camera Sensor ECU
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 time interval of the LKA system
EPS ECU - Final Torque	Monitors the requested torque and validates it against given limits. If value breaches given thresholds a failure is set.
Motor	Applies the requested 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 turned off and Requested Torque 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	LDW turned off and Requested Torque 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	LDW turned off and Requested Torque 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	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 turned off and Requested Torque 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 *frequency* of LDW_Torque_Request sent to the Final Electronic Power Steering Torque component is below Max_Torque_Frequency	C	50 ms	LDW Safety	LDW turned off and Requested Torque set to zero.
Technical Safety Requirement 02	The LDW function shall be deactivated and LDW_Torque_Request shall be set to zero as soon as a failure is detected	C	50 ms	LDW Safety	LDW turned off and Requested Torque set to zero.
Technical Safety Requirement 03	The LDW Safety component shall send a signal to the Car Display ECU to turn on the LED as soon as the LDW function is deactivated	C	50 ms	LDW Safety	LDW turned off and Requested Torque set to zero.
Technical Safety Requirement 04	Validity and integrity of the LDW_Torque_Request signal data transmission shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW turned off and Requested Torque set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the Electronic Power Steering ECU to check for any faults	A	Ignition cycle	Memory Test	LDW turned off and Requested Torque set to zero.

Lane Keeping Assistance (LKA) Requirements:

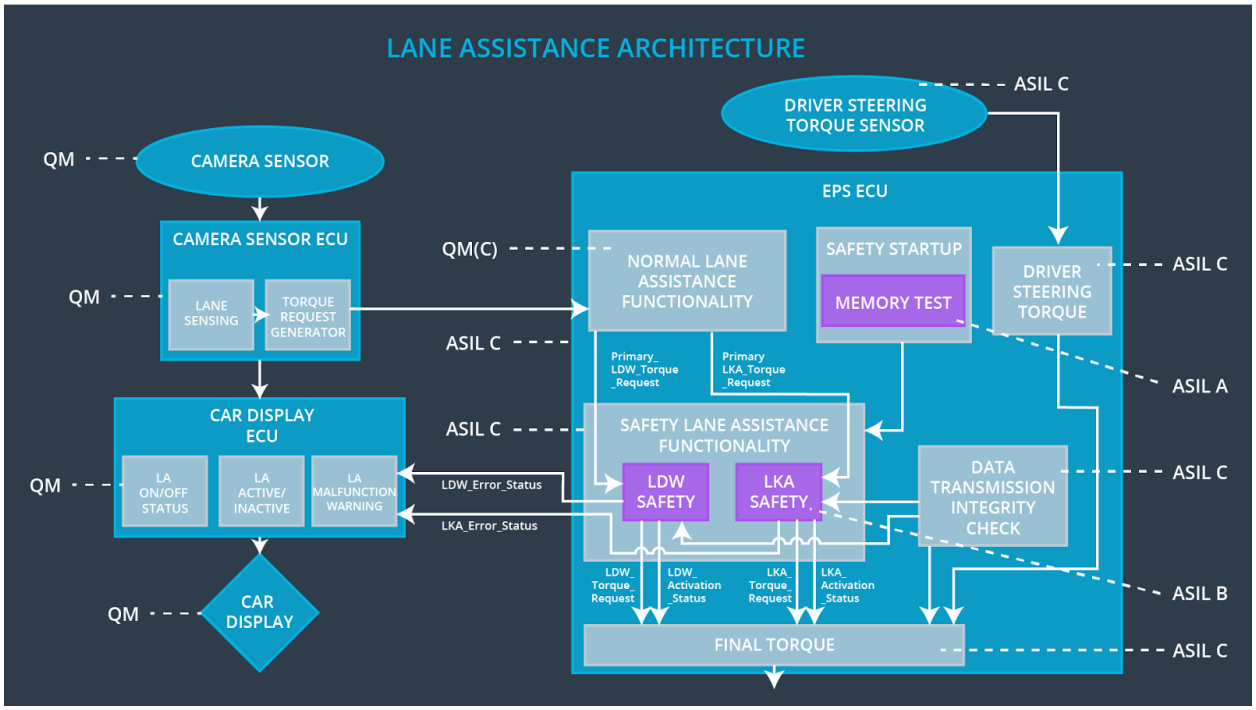
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional 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 amplitude of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	B	500 ms	LKA Safety	LKA turned off and Requested Torque is set to zero
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 turned off and Requested Torque set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by LKA function is shall be deactivated the LKA feature and the LKA_Torque_Request shall be set to zero	B	500 ms	LKA Safety	LKA turned off and Requested Torque set to zero.
Technical Safety Requirement 04	Validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured	B	500 ms	LKA Safety	N/A
Technical Safety Requirement 05	Memory test shall be conducted at start up of the Electronic Power Steering ECU to check for any faults in memory	A	Ignition cycle	Memory Test	LKA turned off and Requested Torque set to zero.

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 is turned of with visual signal on the car display	Max_Torque_Amplitude or Max_Torque_Frequency is exceeded	YES	YES
WDC-02	LKA is turned off with visual signal on the car display	Max_Duration is exceeded	YES	YES