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
26.03.2018	0.1	Stefan Cyliax	Initial version for functional safety project
01.04.2018	1.0	Stefan Cyliax	First RC

Table of Contents

Contents

Purpose of the Technical Safety Concept

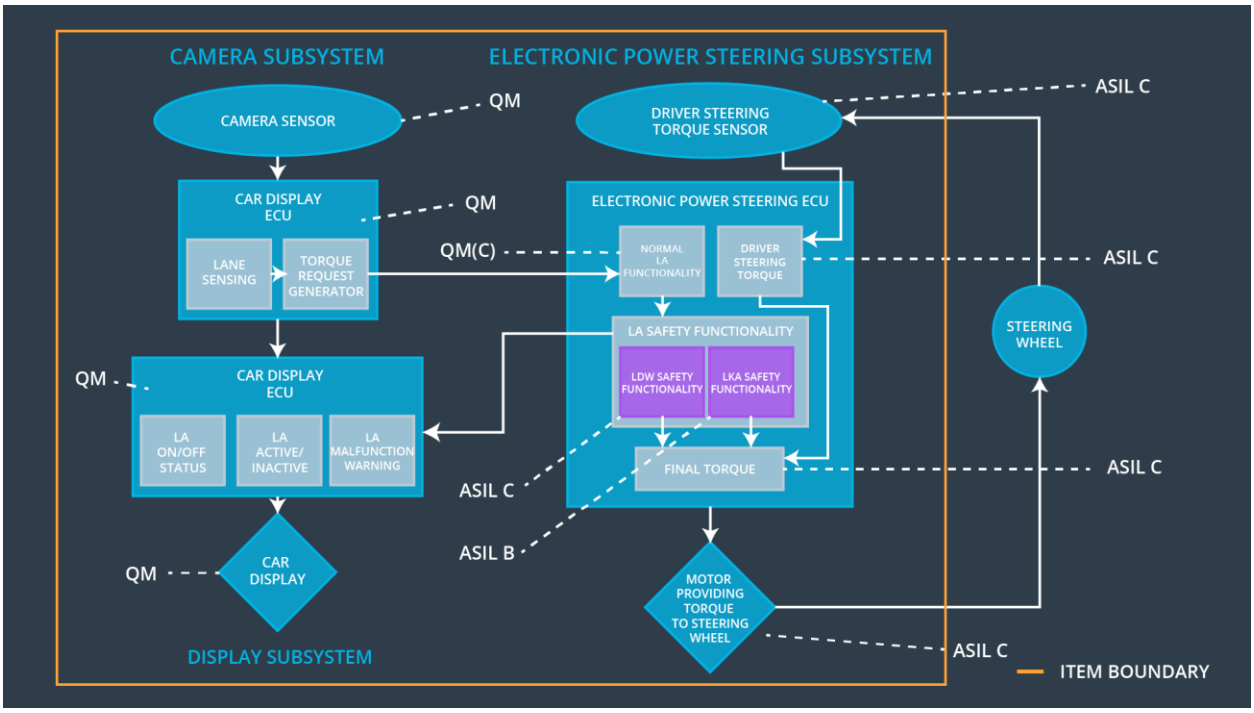
The Purpose of the Technical Safety Concept is to derive technical requirements from the Functional Safety requirements by getting into more detail about the items technology. In contrast to the Functional Safety Concept, it is part of the product development phase.

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 oscillation torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Gradually reduce steering torque to zero
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillation torque frequency is below Max_Torque_Frequency.	C	50 ms	Gradually reduce steering 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	Gradually reduce steering torque to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provides the Camera Display ECU with images of the street in front of the vehicle.
Camera Sensor ECU - Lane Sensing	Detects lane line markers on the camera image and calculates the relative vehicle position to it.
Camera Sensor ECU - Torque request generator	Takes position of the lane line markers and the relative position of the vehicle and creates a correction torque.
Car Display	Displays various information to the driver.
Car Display ECU - Lane Assistance On/Off Status	Provides the Car Display with information of the On/Off state of the Lane Assistance system.
Car Display ECU - Lane Assistant Active/Inactive	Provides the Car Display with information of the Active/Inactive state of the Lane Assistance system.

Car Display ECU - Lane Assistance malfunction warning	Provides the Car Display with information of a possible malfunction of the Lane Assistance system.
Driver Steering Torque Sensor	Senses the current steering torque of the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads the current steering torque of the driver from the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Implements both Lane Assistance functions. Receives torque requests from Camera Sensor ECU and generates steering torque.
EPS ECU - Lane Departure Warning Safety Functionality	Safety module to ensure that torque amplitude and frequency are below maximum.
EPS ECU - Lane Keeping Assistant Safety Functionality	Safety module to ensure that LKA is not activated longer than maximum duration time.
EPS ECU - Final Torque	Combine torque requests from LKA, LDW and Driver Steering Torque to the final torque to be send to the motor.
Motor	Applies the correct torque to the steering wheel of the vehicle.

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_Request = 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_Request = 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_Request = 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_Torque_Request = 0
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	Safety Startup	LDW_Torque_Request = 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 oscillating torque 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	LDW_Torque_Request = 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_Request = 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_Request = 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_Torque_Request = 0
Technical Safety	Memory test shall be conducted at start up of the EPS ECU to check	A	Ignition cycle	Safety Startup	LDW_Torque_R

Requirement 05	for any faults in memory.				equest = 0

Lane Keeping Assistance (LKA) Requirements:

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

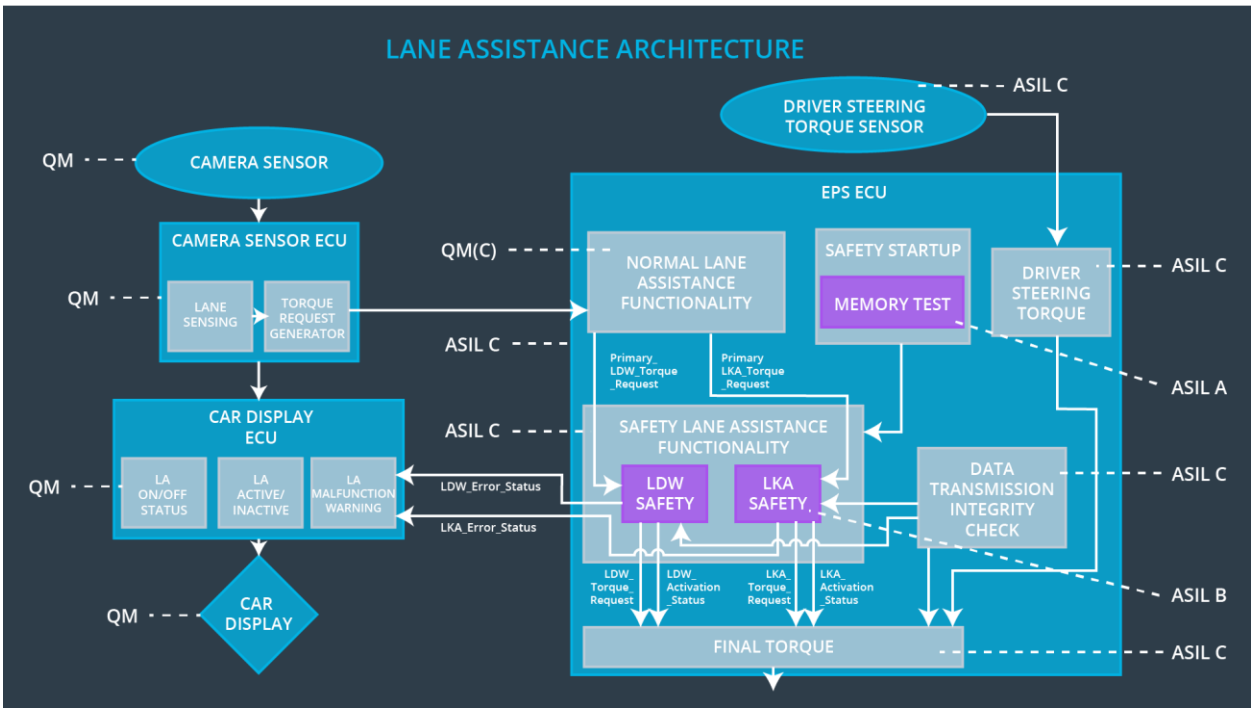
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' is applied for only ‘Max_Duration’.	B	500 ms	LKA_Safety	LKA_Torque_Request = 0
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_Request = 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_Request = 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	LKA_Torque_Request = 0
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	Safety Startup	LKA_Torque_Request = 0

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	LDW_Torque_Request = 0	'LDW_Torque_Request' >= 'Max_Torque_Amplitude. OR 'LDW_Torque_Request' >= 'Max_Torque_Frequency	Yes	Warning on car display
WDC-02	LKA_Torque_Request = 0	‘Max_Duration’ time limit is exceeded.	Yes	Warning on car display