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
23 – May - 2018	1.0	Rajagopala Rao Srinadhuni	Technical Safety Concept expanding the Functional Safety Concepts

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept shall expand upon the functional safety requirements, detailing how each of them shall be realized, through various components and sub-systems present in

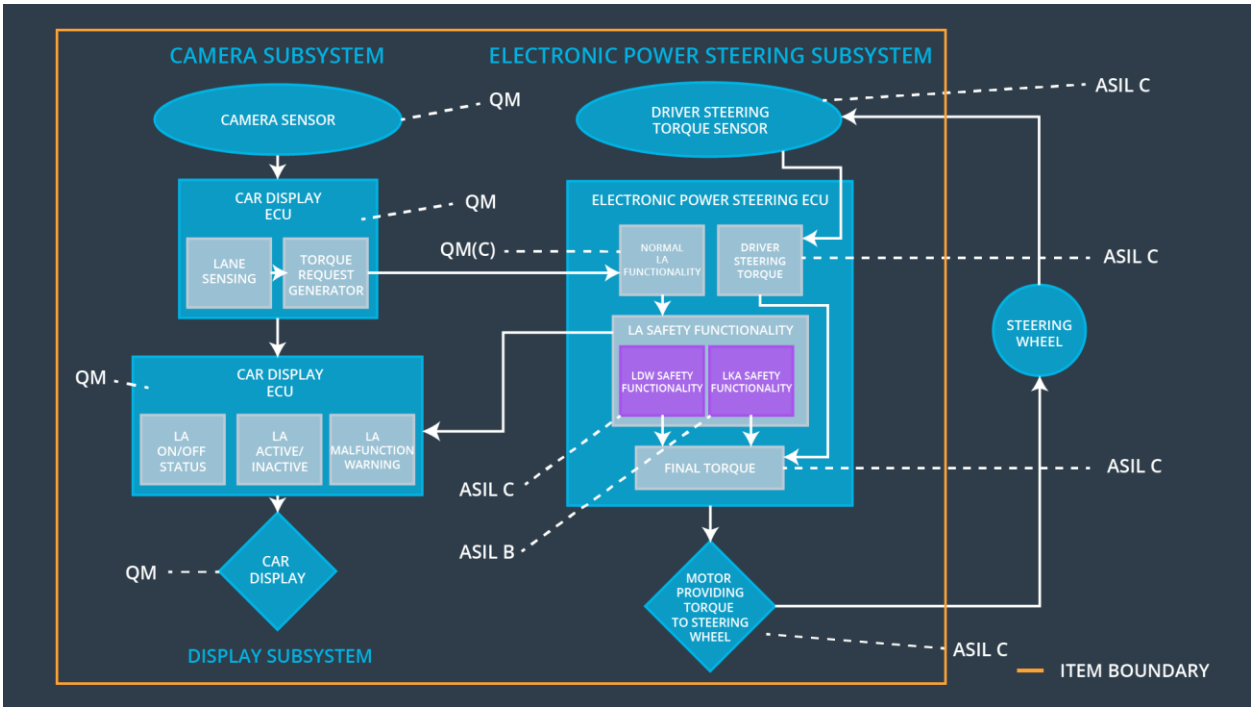
the system. Further, the technical concepts describe what a system shall do when a malfunction violates the safety goal.

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	50ms	Torque_Amplitude reaches zero value
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	50ms	Torque_Frequency reaches zero value
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	500ms	Lane Assist switches off after Max_Duration
Functional Safety Requirement 02-02	The camera sensor ECU shall monitor obstacles as well, included in the detection model	B	30ms	Lane Keeping system shall turn off if not needed
Functional Safety Requirement 02-03	The electronic power steering ECU shall generate steering correction between Min_Correction and Max_Correction value	A	50ms	Correction value settles at zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Takes image feed input for detecting lane change
Camera Sensor ECU - Lane Sensing	Uses learning model or vision techniques to detect when lane change occurs
Camera Sensor ECU - Torque request generator	Generates request for LDW warning through oscillatory torque, for unintended lane changes
Car Display	Gives warning signals for unintentional lane change, high haptic torque, tells if Lane Assistance is active
Car Display ECU - Lane Assistance On/Off Status	Checks and displays if the Lane Assistance System is on
Car Display ECU - Lane Assistant	Checks and displays if the Lane Assistance System

Active/Inactive	is active or inactive
Car Display ECU - Lane Assistance malfunction warning	Checks and displays if the Lane Assistance System gives warning for unintentional lane change
Driver Steering Torque Sensor	Checks if the steering torque is below a fixed maximum
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Sends signal for generating torque which is restricted to a maximum limit below the max_torque
EPS ECU - Normal Lane Assistance Functionality	Generates oscillatory torque for warning driver
EPS ECU - Lane Departure Warning Safety Functionality	Checks if oscillatory torque is within limits and issues warning if not
EPS ECU - Lane Keeping Assistant Safety Functionality	Makes sure lane assistant system is functional only for a fixed duration
EPS ECU - Final Torque	Provides torque signal to steering, post all safety checks
Motor	Performs the rotation necessary for torque

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	Architecture Allocation	Safe State

			Time Interval		
Technical Safety Requirement 01	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final EPS Torque' component is below Max_Torque_Amplitude	C	50ms	LDW Safety Block	Set LDW_Torque_Amplitude zero
Technical Safety Requirement 02	The validity and integrity of the LDW_Torque_Request signal shall be ensured	C	50ms	Data Transmission Integrity Block	Lane Assistance System is turned if Data_Validity is False
Technical Safety Requirement 03	As soon as failure is detected by the LDW function, the LDW_Torque_Request shall be set to zero	C	50ms	LDW Safety Block	Lane Assistance System is turned off
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the software block shall send a signal to turn on a warning light	C	50ms	LA Malfunction Warning Block	Lane Assistance System is turned off with Error_Status True
Technical Safety Requirement 05	Memory tests shall be conducted at the start of EPS ECU to check for any faults in memory	A	Length of ignition cycle	Memory Test Block	Lane Assistance System is turned off

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	The lane keeping item shall	X		

Safety Requirement 01-02	ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency			

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 EPS Torque' component is below Max_Torque_Frequency	C	50ms	LDW Safety Block	Set LDW_Torque_Frequency zero
Technical Safety Requirement 02	The validity and integrity of the LDW_Torque_Request signal shall be ensured	C	50ms	Data Transmission Integrity Block	Lane Assistance System is turned if Data_Validity is False
Technical Safety Requirement 03	As soon as failure is detected by the LDW function, the LDW_Torque_Request shall be set to zero	C	50ms	LDW Safety Block	Lane Assistance System is turned off
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the software block shall send a signal to turn on a warning light	C	50ms	LA Malfunction Warning Block	Lane Assistance System is turned off with Error_Status True
Technical Safety Requirement 05	Memory tests shall be conducted at the start of EPS ECU to check for any faults in memory	A	Length of ignition cycle	Memory Test Block	Lane Assistance System is turned off

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 system shall stop sending LKA_Torque_Request once Max_Duration is completed	B	500ms	LKA Safety Block	Shut down LKA system, as duration > Max_Duration
Technical Safety Requirement 02	The validity and integrity of the LKA_Torque_Request signal shall be ensured	B	500ms	Data Transmission Integrity Block	Lane Assistance System is turned if Data_Validity is False
Technical Safety Requirement 03	As soon as failure is detected by the LKA function, the LKA_Torque_Request shall be set to zero	B	500ms	LKA Safety Block	Lane Assistance System is turned off
Technical Safety Requirement	As soon as the LKA function deactivates the LKA feature,	B	500ms	LA Malfunction Warning Block	Lane Assistance System is

04	the software block shall send a signal to turn on a warning light				turned off with Error_Status True
Technical Safety Requirement 05	Memory tests shall be conducted at the start of EPS ECU to check for any faults in memory	A	Length of ignition cycle	Memory Test Block	Lane Assistance System is turned off

Functional Safety Requirement 02-2 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 02-01	The camera sensor ECU shall monitor obstacles as well, included in the detection model		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	LKA system shall send LKA_Torque_Request to cancel lane change only if No_Obstacle is True	B	30ms	LKA Safety Block	Lane Assistance System is turned off when obstacle present
Technical Safety Requirement 02	The validity and integrity of the LKA_Torque_Request signal shall be ensured	B	30ms	Data Transmission Integrity Block	Lane Assistance System is turned if Data_Validity is False
Technical Safety	As soon as failure is detected by the LKA function, the	B	30ms	LKA Safety Block	Lane Assistance

Requirement 03	LKA_Torque_Request shall be set to zero				System is turned off
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the software block shall send a signal to turn on a warning light	B	30ms	LA Malfunction Warning Block	Lane Assistance System is turned off with Error_Status True
Technical Safety Requirement 05	Memory tests shall be conducted at the start of EPS ECU to check for any faults in memory	A	Length of ignition cycle	Memory Test Block	Lane Assistance System is turned off

Functional Safety Requirement 02-3 with its associated system elements (derived in the functional safety concept)

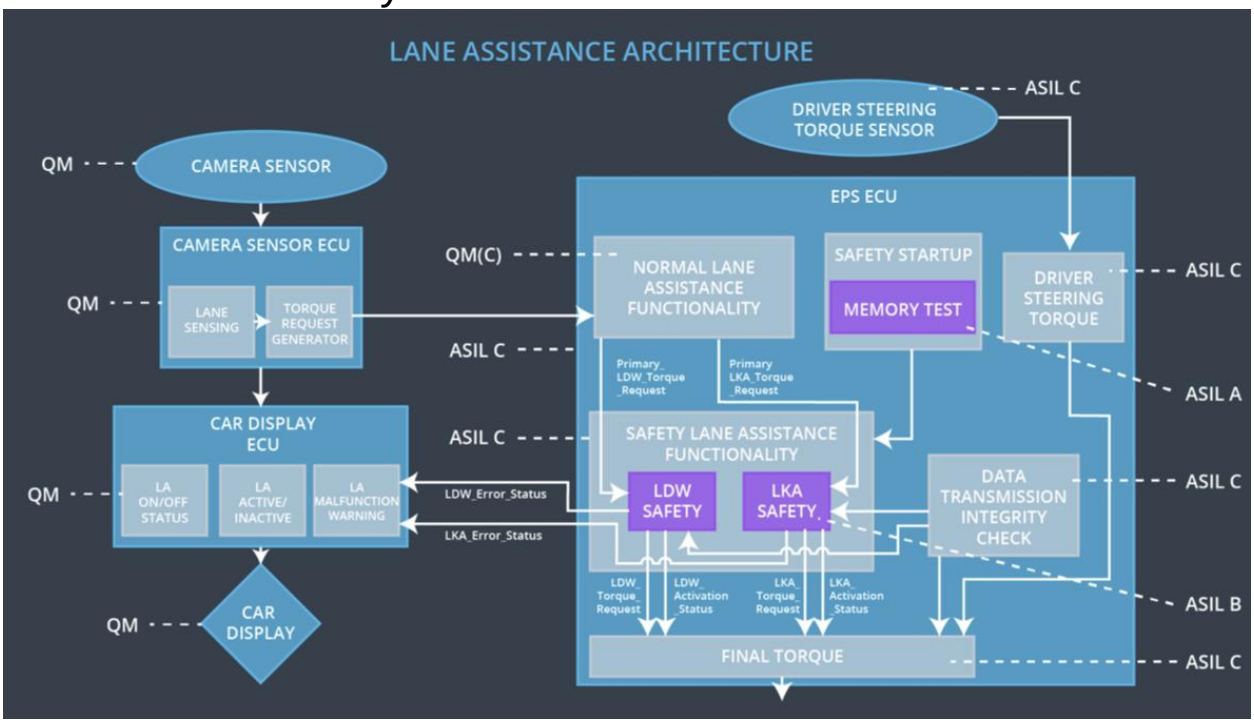
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The electronic power steering ECU shall generate steering correction between Min_Correction and Max_Correction value	X		

Technical Safety Requirements related to Functional Safety Requirement 02-03 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA system shall LKA_Torque_Request between Min_Correction and Max_Correction value based on Terrain_Type	A	50ms	LKA Safety Block	LKA_Torque_Request >= Min_Correction and LKA_Torque_Request <=Max_Correction depending on Terrain_Type

Technical Safety Requirement 02	The validity and integrity of the LKA_Torque_Request signal shall be ensured	A	50ms	Data Transmission Integrity Block	Lane Assistance System is turned if Data_Validity is False
Technical Safety Requirement 03	As soon as failure is detected by the LKA function, the LKA_Torque_Request shall be set to zero	A	50ms	LKA Safety Block	Lane Assistance System is turned off
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the software block shall send a signal to turn on a warning light	A	50ms	LA Malfunction Warning Block	Lane Assistance System is turned off with Error_Status True
Technical Safety Requirement 05	Memory tests shall be conducted at the start of EPS ECU to check for any faults in memory	A	Length of ignition cycle	Memory Test Block	Lane Assistance System is turned off

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All requirements save requirements for Functional Requirement 2-02 depend on the EPS ECU system. The remaining requirement depends on the EPS ECU as well, with a change only in the training phase of the deep learning model for the Camera Sensor ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Shut down	Malfunction_01 Malfunction_02	Yes	Indicator lamp, indicating maximum torque
WDC-02	Shut down	Malfunction_03	Yes	Indicator lamp blinks twice as system turns off

WDC-03	Shut down	Malfunction_04	Yes	Different shades in indicator lamp, conveying excess or insufficient corrective measure
WDC-04	Shut down	Malfunction_05	Yes	Indicator lamp blinks twice as system turns off