Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
13.12.2017	1.0	Dhanasekaran	Initial Version
18.12.2017	2.0	Dhanasekaran	Update based on Udacity review comments

Table of Contents

Purpose of the Technical Safety Concept

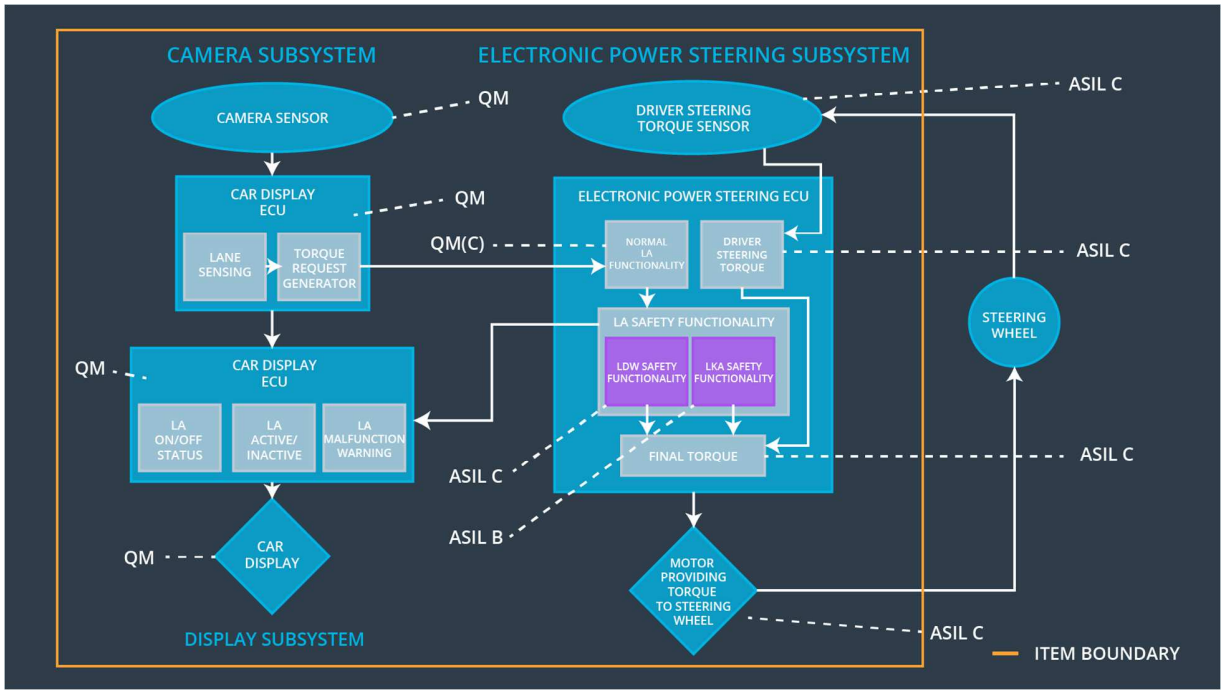
The purpose of this document is to derive the technical safety requirement from functional safety requirement and allocate them to system architectural elements

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	Switch off LDW functionality
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	Switch off LDW functionality
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	Switch off LKA functionality
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the additional lane keeping assistance torque is applied in the same direction as steering wheel movement	C	50ms	Switch off LKA functionality

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Takes images of the road
Camera Sensor ECU - Lane Sensing	Senses whether vehicle is within the lane or not
Camera Sensor ECU - Torque request generator	Generates torque request if vehicle is deviating from the ego lane
Car Display	Displays warning and status regarding Lane assistance functionality
Car Display ECU - Lane Assistance On/Off Status	Displays the ON/OFF status of the lane assistance function
Car Display ECU - Lane Assistant Active/Inactive	Displays the Active/Inactive status of the lane assistance function
Car Display ECU - Lane Assistance	Display warning is the lane assistance function has

malfunction warning	malfunctions
Driver Steering Torque Sensor	Measures the actual torque at the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Calculates required steering torque
EPS ECU - Normal Lane Assistance Functionality	Non-safety relevant lane assistance functionality
EPS ECU - Lane Departure Warning Safety Functionality	Implements the LDW safety functionality
EPS ECU - Lane Keeping Assistant Safety Functionality	Implements LKS safety functionality
EPS ECU - Final Torque	Calculates the final steering torque
Motor	Provides the 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	50ms	LDW_Safety software component	The LDW torque amplitude request shall be 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	50ms	LDW_Safety software component	The LDW torque amplitude request shall be 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	50ms	LDW_Safety software component	The LDW torque amplitude request shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data transmission integrity check	The LDW torque amplitude request shall be set to zero
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	The LDW torque amplitude request shall be 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 the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency'	C	50ms	LDW_Safety software component	The LDW torque Frequency request shall be 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	50ms	LDW_Safety software component	The LDW torque Frequency request shall be 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	50ms	LDW_Safety software component	The LDW torque Frequency request shall be set to zero

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data transmission integrity check	The LDW torque Frequency request shall be set to zero
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	The LDW torque Frequency request shall be 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		

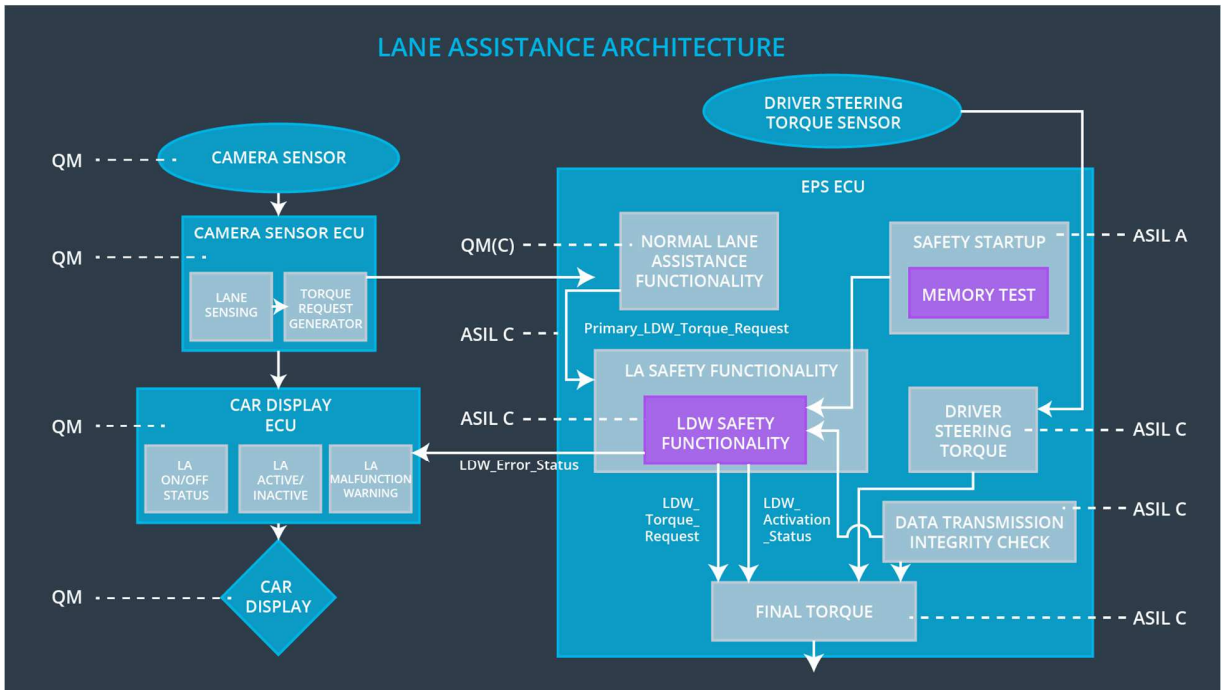
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 'LKA_Torque_Request' is sent to 'Final electronic power steering Torque' only for Max_Duration time	B	500ms	LKA_Safety software component	The LKA torque shall be set to zero
Technical Safety	As soon as the LKA function deactivates the LKA feature, the	B	500ms	LKA_Safety	The LKA

Requirement 02	'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light			software component	torque shall be set to zero
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	LKA_Safety software component	The LKA torque shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Data transmission integrity check	The LKA torque shall be set to zero
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	The LKA torque shall be set to zero

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

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All Technical safety requirements are allocated to Electronic Power Steering ECU

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the LDW functionality	When the following functional safety requirements are not met “Functional Safety Requirement 01-01” “Functional Safety Requirement 01-02”	Yes	A blinking warning signal is displayed in the instrument cluster and an acoustic warning is also provided
WDC-02	Turn off the LKA functionality	When the following functional safety requirements are not met “Functional Safety Requirement 02-01” “Functional Safety Requirement 02-02” “Functional Safety Requirement 02-03”	Yes	A blinking warning signal is displayed in the instrument cluster and an acoustic warning is also provided