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
22/05/2018	0.1	Kapil Saini	Initial draft
23/05/2018	1.0	Kapil Saini	Finalized version

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to specify the roadmap for implementation of the defined functional safety concept. This includes concrete information on item's technology.

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 lane keeping item shall ensure that the lane departure warning torque **amplitude** is below **Max_Torque_Amplitude**	C	50ms	Turn off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning torque **frequency** is below **Max_Torque_Frequency**	C	50ms	Turn off LDW
Functional Safety Requirement 02-01	Ensure that LKA torque is applied only for a limited time not more than **Max_Duration**	B	500ms	Turn off LKA setting torque to zero

Refined System Architecture from Functional Safety Concept

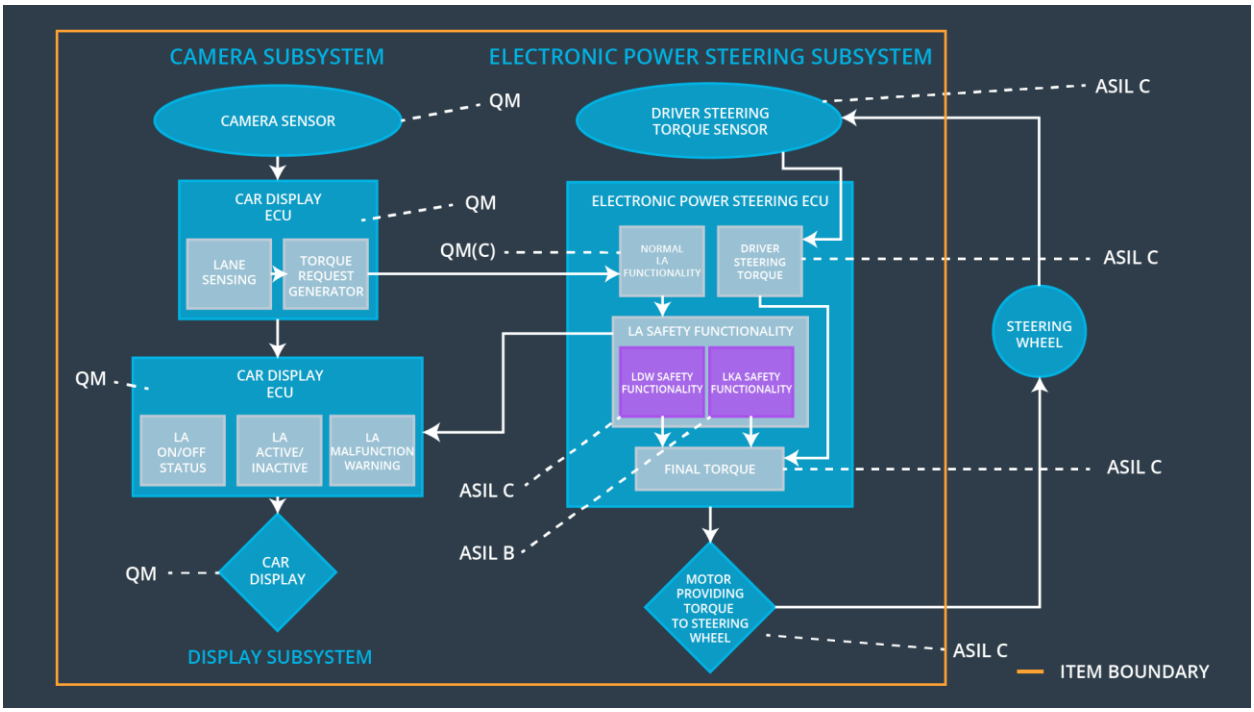

Figure 1Refined System Architecture

Functional overview of architecture elements

Element	Description
Camera Sensor	Sensors to capture environmental information as images and provide them to the camera sensor ECU continuously.
Camera Sensor ECU - Lane Sensing	A processor unit to process acquired images by camera sensors to detect Lane Lines and calculate car positions w.r.t. to lane lines.
Camera Sensor ECU - Torque request generator	A processor unit to generate Torque request to the car for the Electronic Power Steering ECU
Car Display	Display device to display system status and warnings during system malfunctions to driver.
Car Display ECU - Lane Assistance On/Off Status	A control function to display on/off status of lane assistance system.
Car Display ECU - Lane Assistant	A control function to display active/inactive status of

Active/Inactive	lane assistance system.
Car Display ECU - Lane Assistance malfunction warning	Function to display any malfunction in the Lane Assistance system
Driver Steering Torque Sensor	Sensor to measures the torque applied to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Processing unit to process input from driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	A function to process the data from the torque request generator
EPS ECU - Lane Departure Warning Safety Functionality	A function to ensure the LDW safety functionality
EPS ECU - Lane Keeping Assistant Safety Functionality	Function to check for any malfunction in the Lane Keeping Assistance system.
EPS ECU - Final Torque	Combine the inputs from LDW and LKA and deliver the final torque request to the motor
Motor	An electric motor that interpret the EPS ECU data to control 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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is	X		

01-01	below Max_Torque_Amplitude			

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	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	50ms	LDW Safety	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	50ms	LDW Safety	Torque_Request=0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data Transmission Integrety Check	Torque_Request=0
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	50ms	Memory test	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 Frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50ms	LDW safety	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	50ms	LDW safety	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	50ms	LDW safety	Torque_Request=0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall	c	50ms	Data Transmission Integrety Check	Torque_Request=0

	be ensured				
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	50ms	Memory Check	Torque_ Request =0

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 LKA safety component shall ensure that the Duration of LKA Torque application is less than Max_Duration.	B	500ms	LKA Safety	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.	B	500ms	LKA Safety	Torque_Request=0
Technical	As soon as a failure is detected	B	500ms	LKA Safety	Torque_Re

Safety Requirement 03	by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero.				quest=0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	B	500ms	Data Transmission Integrety Check	Torque_Request=0
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	500ms	Memory Check	Torque_Request=0

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

Refinement of the System Architecture

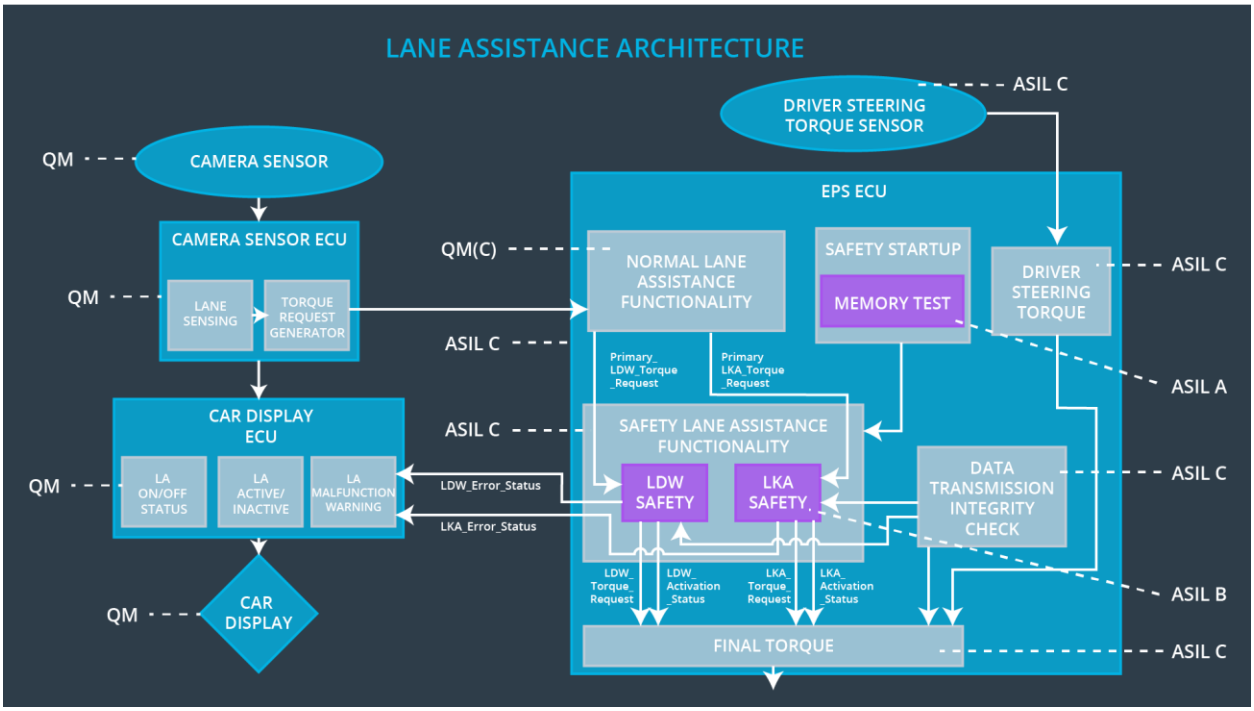

Figure 2 Refined Lane System Architecture

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	Turn off the functionality	**Malfunction_01** Is_Max_Torque_ Exceeded “Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback”	Yes	Turn on warning light on car display and dashboard.
WDC-02	Turn off the functionality	**Malfunction_02** Is_Max_Duration _Exceeded “Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback”	Yes	Turn on warning light on car display and dashboard