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
03/03/2019	1.0	Rangarajan Ramanujam	Initial draft

Table of Contents

Purpose of the Technical Safety Concept

This document defines new requirements and assigns it to the system architecture. These requirements are more concrete and gets into details of the item’s technology as specified by ISO 26262.

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 oscillating torque amplitude is below Max_torque_Amplitude	C	50 mS	LDW Torque amplitude is set to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 mS	LDW Torque amplitude is set to zero
Functional Safety Requirement 01-03	The lane keeping item shall ensure that the lane departure oscillating torque will be turned off when the driver is applying more than Max_Driver_Torque_Amplitude	B	20 mS	LDW Torque amplitude is set to zero
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only for Max_Duration	B	500 mS	Lane Keeping Assistance Torque is zero
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the Lane Keeping Assistance shall be deactivated under braking conditions	A	50 mS	Lane Keeping Assistance Torque is zero

Refined System Architecture from Functional Safety Concept

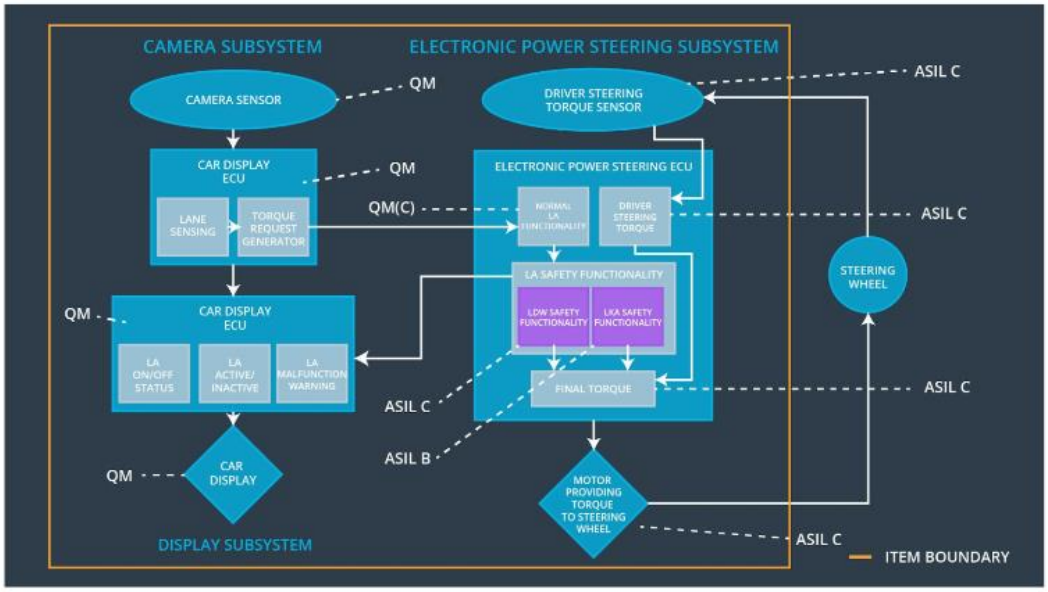

Fig 1: Refined Lane Assistance System Architecture

Functional overview of architecture elements

Element	Description
Camera Sensor	Capture road images and provide them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Software module detecting the lane line positions from the Camera Sensor images
Camera Sensor ECU - Torque request generator	Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU
Car Display	Displays warning to the driver
Car Display ECU - Lane Assistance On/Off Status	Indicate the status of the Lane Assistance functionality (ON/OFF)
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive)
Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction on the Lane Assistance functionality
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the driver’s torque request from the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Software module receiving the Camera Sensor ECU Torque request
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude ,torque Frequency is below Max_Torque_Frequency and warning is turned off when the driver input is more than a Max_Driver_Torque_Amplitude
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not active more than Max Duration time and the assistance functionality is turned off during braking conditions.
EPS ECU - Final Torque	Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor
Motor	Applies the required torque to the steering wheels

Technical Safety Concept

Technical Safety Requirements

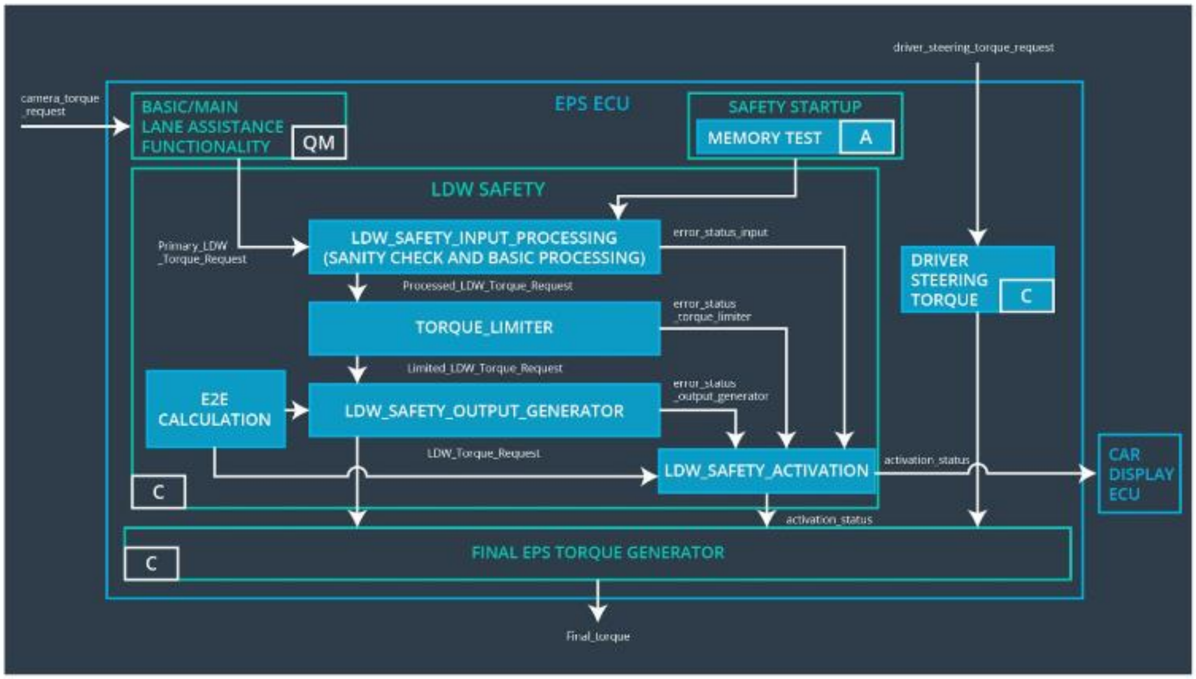
driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
DRIVER STEERING TORQUE
C
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

Fig 2: Refined Lane Assistance System Architecture

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 Lane Departure Warning 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 Amplitude shall be set to zero
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal	C	50 mS	LDW Safety	LDW Torque Request Amplitude shall be set to zero
Technical Safety Requirement 03	When 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 Amplitude 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	50 mS	LDW Safety	LDW Torque Request Amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	LDQ Torque Request Amplitude 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**	**A S I L**	**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	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero
Technical Safety Requirement 02	The validity and the integrity of the data transmission for ‘Max_Torque_Frequency’ signal shall be ensured	C	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero
Technical Safety Requirement 03	When a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘Max_Torque_Frequency’ shall be set to zero	C	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero
Technical Safety Requirement 04	When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal	C	50 mS	LDW Safety	LDW Torque Request Frequency shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	LDW Torque Request Frequency shall be set to zero

Functional Safety Requirement 01-3 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 01-02	The lane keeping item shall ensure that the lane departure oscillating torque will be turned off when the driver is applying more than Max_Driver_Torque_Amplitude	X		

Technical Safety Requirements related to Functional Safety Requirement 01-03 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 and frequency of 'LDW_Torque_Request' and 'Max_Torque_Frequency' shall be set to zero when driver torque input is greater than 'Max_Driver_Torque_Amplitude'	B	20 mS	LDW Safety	LDW Torque Request Amplitude and Frequency shall be set to zero
Technical Safety Requirement 02	When the driver torque input is greater than the 'Max_Driver_Torque_Amplitude', the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a 'LDW_Inactive' signal	B	20 mS	LDW Safety	LDW Torque Request Amplitude and Frequency shall be set to zero
Technical Safety Requirement 03	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	LDW Torque Request Amplitude and Frequency 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 the duration of the lane keeping assistance torque is applied for less than 'Max_Duration'	B	500 mS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	B	500 mS	LKA Safety	Lane Keeping Assistance Torque is 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	500 mS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 04	When the LKA feature is deactivated, 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	Lane Keeping Assistance Torque is set to zero
Technical Safety	Memory test shall be conducted at startup of the	A	Ignition Cycle	Data Transmission	Lane Keeping

Requirement 05	EPS ECU to check for any faults in memory			Integrity Check	Assistance torque is set to zero

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 02-02	The electronic power steering ECU shall ensure that the Lane Keeping Assistance shall be deactivated under braking conditions	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	The LKA Safety Component shall ensure the 'LKA_Torque_Request' is set to zero under braking conditions	A	50 mS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 02	When there is heavy braking conditions, the ‘LKA Safety’ software module shall send a signal to the Car Display ECU to turn on a ‘LKA_Inactive’ signal	A	50 mS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 03	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	A	Ignition Cycle	Data Transmission Integrity Check	Lane Keeping Assistance torque is set to zero

Refinement of the System Architecture

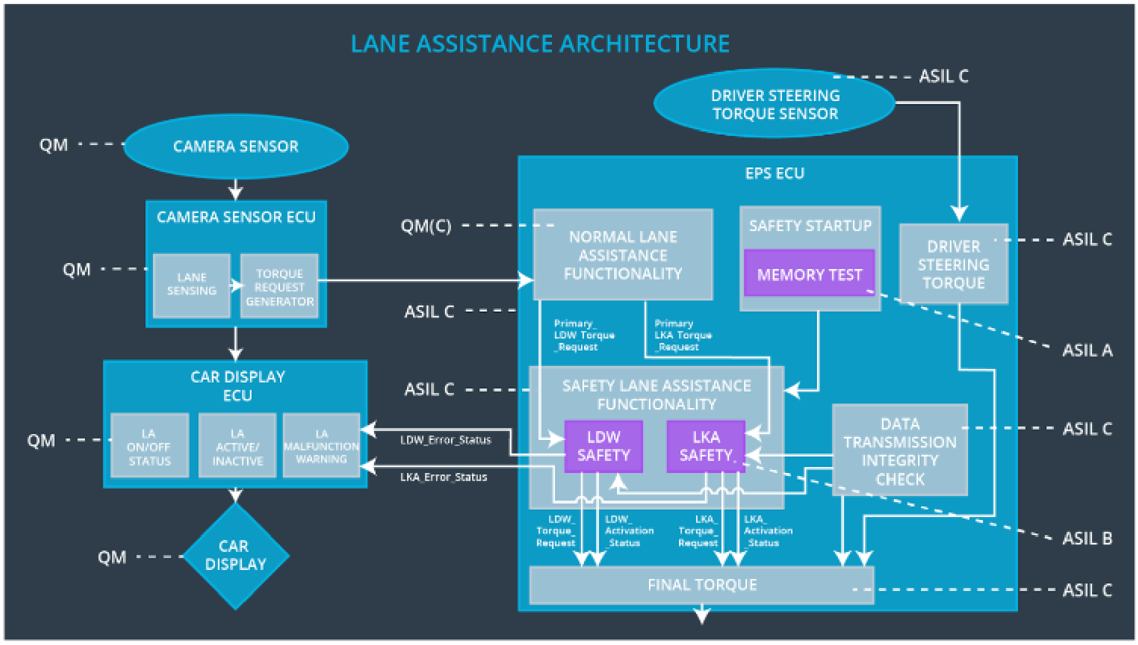

Fig 2: Further Refinement - Lane Assistance Architecture

Allocation of Technical Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The Lane Departure Warning 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’	X		
Technical Safety Requirement 01-01-02	When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal	X		
Technical	When a failure is detected by the	X		

Safety Requirement 01-01-03	LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall be set to zero			
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	X		
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	X		
Technical Safety Requirement 01-02-01	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'	X		
Technical Safety Requirement 01-02-02	The validity and the integrity of the data transmission for 'Max_Torque_Frequency' signal shall be ensured	X		
Technical Safety Requirement 01-02-03	When a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'Max_Torque_Frequency' shall be set to zero	X		
Technical Safety Requirement 01-02-04	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal	X		
Technical Safety Requirement 01-02-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	X		
Technical Safety Requirement	The LDW Safety component shall ensure that the amplitude and	X		

01-03-01	frequency of ‘LDW_Torque_Request’ and ‘Max_Torque_Frequency’ shall be set to zero when driver torque input is greater than ‘Max_Driver_Torque_Amplitude’			
Technical Safety Requirement 01-03-02	When the driver torque input is greater than the ‘Max_Driver_Torque_Amplitude’, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a ‘LDW_Inactive’ signal	X		
Technical Safety Requirement 01-03-04	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	X		
Technical Safety Requirement 02-01-01	The LKA Safety Component shall ensure the duration of the lane keeping assistance torque is applied for less than ‘Max_Duration’	X		
Technical Safety Requirement 02-01-02	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured	X		
Technical Safety Requirement 02-01-03	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	X		
Technical Safety Requirement 02-01-04	When the LKA feature is deactivated, the LKA Safety software block shall send a signal to the car display ECU to turn on a warning light	X		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	X		

TechnicalSafety Requirement 02-02-01	The LKA Safety Component shall ensure the 'LKA_Torque_Request' is set to zero under braking conditions	X		
Technical Safety Requirement 02-02-02	When there is heavy braking conditions, the ‘LKA Safety’ software module shall send a signal to the Car Display ECU to turn on a ‘LKA_Inactive’ signal	X		
Technical Safety Requirement 02-02-03	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory	X		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off system	Malfunction_01, Malfunction_02, Malfunction_05	Yes	Warning Light on the dashboard
WDC-02	Turn off system	Malfunction 03, Malfunction 04	Yes	Warning Light on the dashboard