



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	Ujjwal Saxena	Initial draft
24/05/2018	1.0	Ujjwal Saxena	Finalized version

# Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose of the Technical Safety Concept](#)

[Inputs to the Technical Safety Concept](#)

[Functional Safety Requirements](#)

[Refined System Architecture from Functional Safety Concept](#)

[Functional overview of architecture elements](#)

[Technical Safety Concept](#)

[Technical Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Technical Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

# 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	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure warning torque <b>amplitude</b> is below <b>Max_Torque_Amplitude</b>	C	50ms	Turn off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning torque <b>frequency</b> is below <b>Max_Torque_Frequency</b>	C	50ms	Turn off LDW
Functional Safety Requirement 02-01	Ensure that LKA torque is applied only for a limited time not more than <b>Max_Duration</b>	B	500ms	Turn off LKA setting torque to zero

## Refined System Architecture from Functional Safety Concept

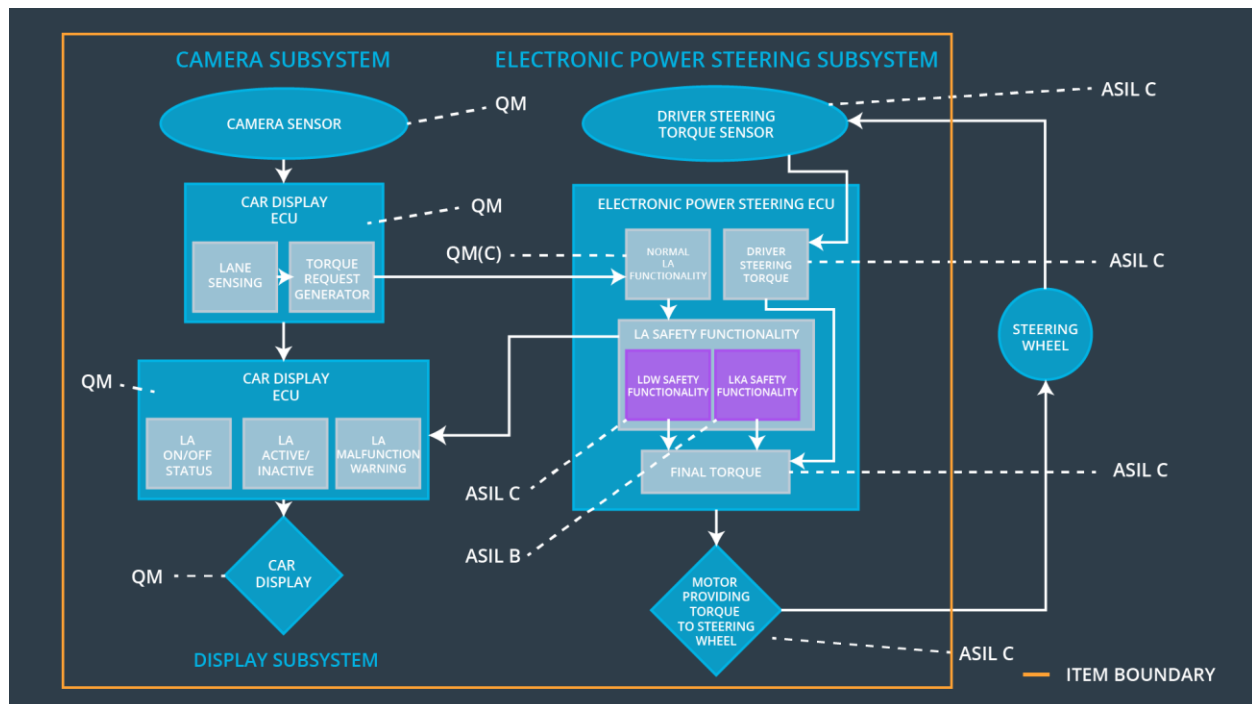


Figure 1 Refined System Architecture

## 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	Checks for any malfunction in the Lane Departure Warning function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn't any malfunction)
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks for any malfunction in the Lane Keeping Assistance function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn't any malfunction)
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 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	As soon as the 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 block	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature , 'LDW safety' software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety block	Lane Departure Warning Torque Request Amplitude 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	The length of ignition cycle	Data Transmission Integrity Check	Lane Departure Warning 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 block	Lane Departure Warning Torque Request Amplitude

					shall be set to zero.
Technical Safety Requirement 05	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 block	Lane Departure Warning 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	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	As soon as the 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 block	Lane Departure Warning Torque Request Frequency shall be set to zero.



Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature , 'LDW safety' software block shall send a signal to the car display ECU to turn on a warning light	C	50 ms	LDW Safety block	Lane Departure Warning Torque Request 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	The length of ignition cycle	Data Transmission Integrity Check	Lane Departure Warning Torque Request Frequency 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 block	Lane Departure Warning Torque Request Frequency shall be set to zero
Technical Safety Requirement 05	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_Frequency'.	C	50 ms	LDW Safety block	Lane Departure Warning Torque Request 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	As soon as the 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 block	Lane Keeping Assistance Torque Request shall be set to zero
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature , 'LKA safety' software block shall send a signal to the car display ECU to turn on a warning light	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request 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	The length of ignition cycle	Data Transmission Integrity Check	Lane Keeping Assistance Torque Request 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	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request shall be set to zero
Technical Safety Requirement 05	The LKA safety component shall ensure that duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request shall be set to zero

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn OFF the Functionality	Malfunction_01 Malfunction_02	Yes	Warning Light on Dashboard and warnings displayed on car display
WDC-02	Turn OFF the Functionality	Malfunction_03	Yes	Warning Light on Dashboard and warnings displayed on car display

