



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
3/13/18	1	Scott Schnelle	First draft of Technical Safety Concept

## 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

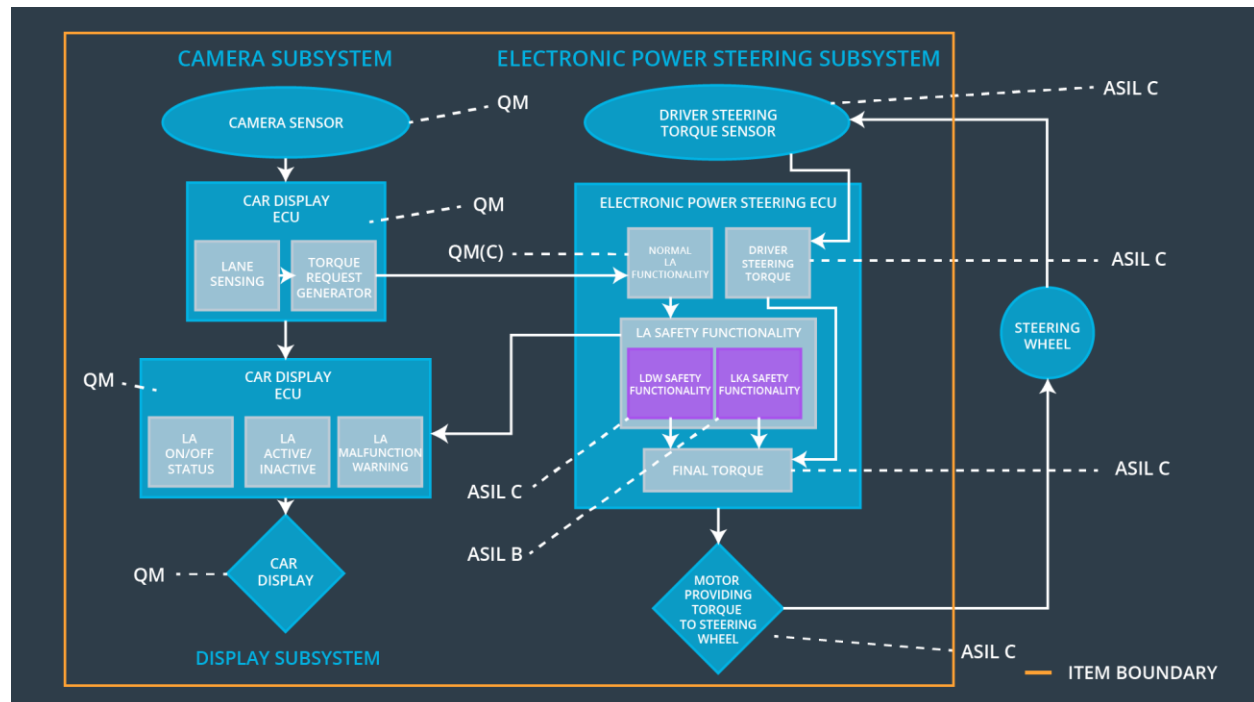
The purpose of the Technical Safety Concept is to define and assign safety requirements to the system architecture. These requirements are very specific and detailed for each part of the systems technology as specified by ISO 26262.

# 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.

## Refined System Architecture from Functional Safety Concept

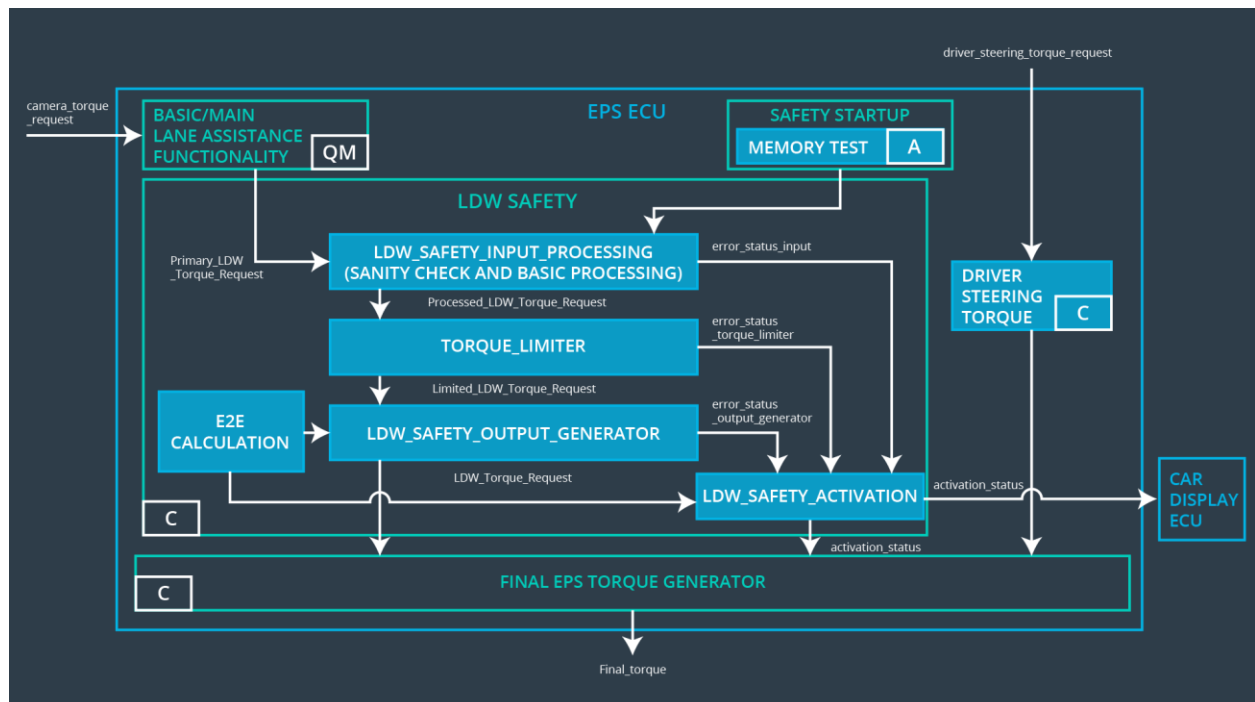


## Functional overview of architecture elements

Element	Description
Camera Sensor	Capture road images
Camera Sensor ECU - Lane Sensing	Analyze road images for vehicle/lane localization
Camera Sensor ECU - Torque request generator	Request a torque based on current vehicle position
Car Display	Provide the display with what systems are active
Car Display ECU - Lane Assistance On/Off Status	Show the driver if the LA is on or off
Car Display ECU - Lane Assistant Active/Inactive	Show the driver if the LA is active or not
Car Display ECU - Lane Assistance malfunction warning	Show the driver if the LA is malfunctioning
Driver Steering Torque Sensor	Measure driver steering torque

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receive driver steering torque
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 and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not activate more than Max_duration time.
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

### 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 01-01-01	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.'	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
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.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical	The validity and integrity of the	C	50 ms	LDW Safety	Lane

Safety Requirement 01-01-04	data transmission for 'LDW_Torque_Request' signal shall be ensured.				Departure Warning torque to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque 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 01-02-01	The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.

**Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:**

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
----	---	---

Technical Safety Requirement 01-01-01	Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation	Verify the Lane Departure Warning functionality is turned off.
Technical Safety Requirement 01-01-02	Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION.	Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal.
Technical Safety Requirement 01-01-03	Validate the 'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero.	Verify the Final EPS Torque generator receives a LDW_Torque_Request of zero.
Technical Safety Requirement 01-01-04	Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.
Technical Safety Requirement 01-01-05	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails.
Technical Safety Requirement 01-02-01	Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria.	Verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds Max_Torque_Request.

### 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:

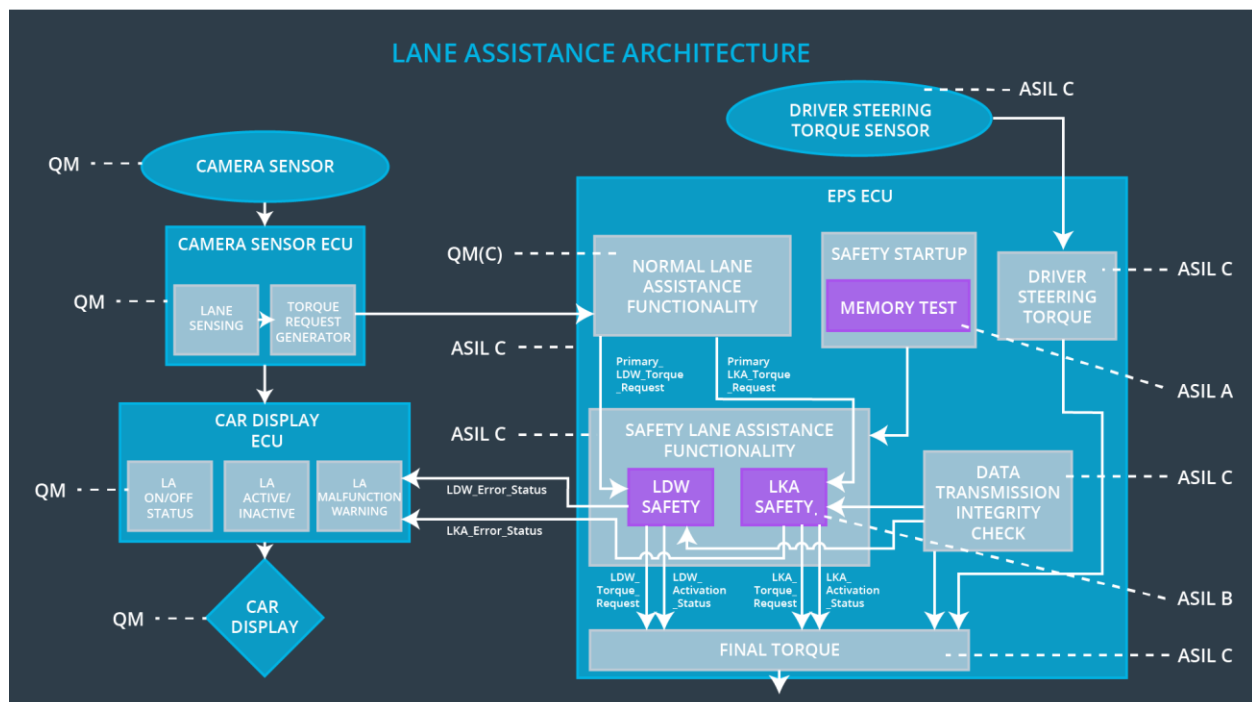
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-01	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-02	When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-03	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-01-01	Validate the Max_Duration is set to the chosen value from LKA Validation Assistance Criteria	Verify the functionality is turned off after it is applied for Max_Duration.
Technical	Validate the 'TORQUE_LIMITER'	Verify the Car Display ECU displays

Safety Requirement 02-01-02	sends the error_status_torque_limiter signal to the LKA_SAFETY_ACTIVATION.	the Lane Keeping Assistance malfunction warning signal.
Technical Safety Requirement 02-01-03	Validate the 'TORQUE_LIMITER' sends 'LKA_Torque_Request' with zero.	Verify the Final EPS Torque generator receives a LKA_Torque_Request of zero.
Technical Safety Requirement 02-01-04	Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.
Technical Safety Requirement 02-01-05	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify the Lane Keeping Assistance is turned off when the Safety Startup Memory fails.

## Refinement of the System Architecture



## Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical 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 Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	X		
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 start up of the EPS ECU to check for any memory problems	X		
Technical Safety Requirement 01-02-01	The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power	X		

	steering Torque' component is below 'Max_Torque_Frequency.'			
Technical Safety Requirement 02-01-01	The Lane Keeping Assistance 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	When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.	X		
Technical Safety Requirement 02-01-03	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.	X		
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	X		
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems			

## Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance

	Assistance functionality			Malfunction Warning on Car Display
--	-----------------------------	--	--	--