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
04 Sep 2017	1.0	Navneet Latawa	First submission
20 Sep 2017	2.0	Navneet Latawa	• Added 4 Technical Safety Requirements for *Functional Safety Requirement 01-02* • For Technical Safety Requirement 01, 02, 03, Architecture Allocation is set to "LKA Safety block".

Table of Contents

Purpose of the Technical Safety Concept

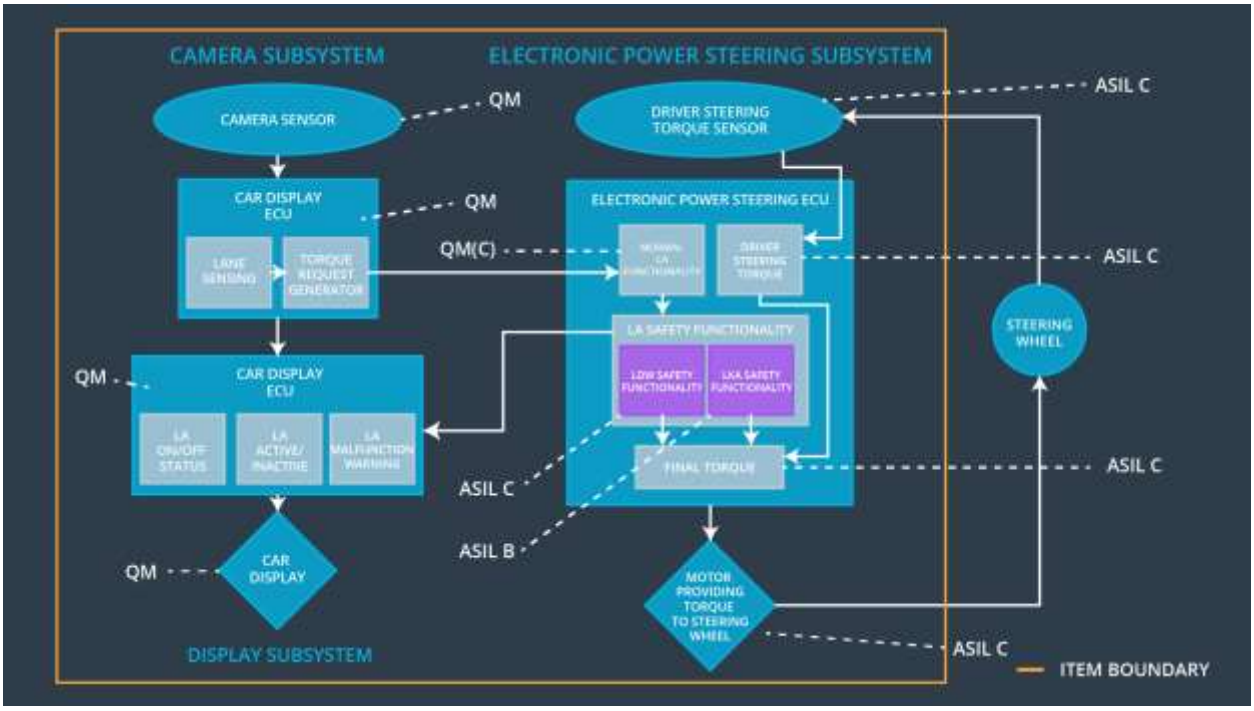
The purpose of Technical Safety Concept is to turn Functional Safety Requirements to Technical Safety Requirements and allocating Technical Safety Requirements to the system architecture.

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	The electronic power steering ECU reduces the oscillating torque amplitude to zero.
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	The electronic power steering ECU reduces the oscillating torque frequency to zero.
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	The electronic power steering ECU reduces the oscillating torque to zero.

Refined System Architecture from Functional Safety Concept



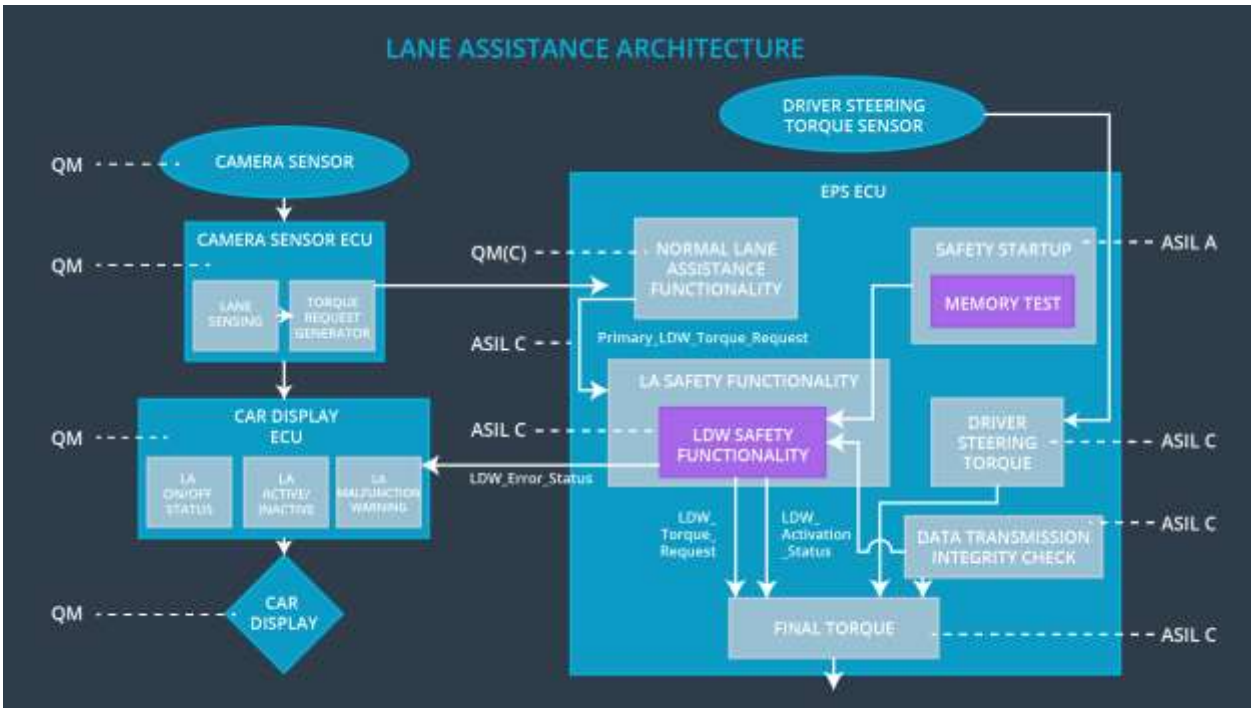
Functional overview of architecture elements

Element	Description
Camera Sensor	It is a sensor hardware that captures information related to lane lines
Camera Sensor ECU - Lane Sensing	This is a software unit that does calculations related to lane sensing and lane departures.
Camera Sensor ECU - Torque request generator	This is a software unit that does calculations to find the amount of torque to be generated to avoid lane departures and keeping car in lane.
Car Display	The visual display panel where warnings and activations\deactivations are reported and which has LKA on/off switch.
Car Display ECU - Lane Assistance On/Off Status	Visual display to indicate whether LKA is on or off.
Car Display ECU - Lane Assistant Active/Inactive	Visual display to indicate whether LKA is currently active or inactive..
Car Display ECU - Lane Assistance malfunction warning	Visual display showing any malfunction in Lane Assistance system(Both LKA, LDW).
Driver Steering Torque Sensor	The hardware sensor unit determining the amount of torque driver is applying.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Software module responsible for doing calculations related to the torque applied by the driver.
EPS ECU - Normal Lane Assistance Functionality	The software module connected to the EPS and responsible for doing calculations related to the torque needed during normal lane operation of the car i.e, when only driver is providing torque.
EPS ECU - Lane Departure Warning Safety Functionality	The software module connected to the EPS and responsible for doing calculations related to the torque to be applied to avoid the vehicle from departing lanes(LDW functionality).
EPS ECU - Lane Keeping Assistant Safety Functionality	The software module connected to the EPS and responsible for doing calculations related to the torque to be applied to keep the vehicle in lane(

	LKA functionality).
EPS ECU - Final Torque	The software module connected to the EPS and responsible for calculating final torque value to be sent to the motor to provide LDW and LKA funtionality.
Motor	The hardware unit providing actual physical torque to the steering.

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 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 block	LDW torque output is set to zero.
Technical Safety Requirement 01-01-02	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 block	LDW torque output is set to zero.
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request'	C	50ms	LDW Safety block	LDW torque output is set to zero.

	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.	C	50ms	Data Transmission Integrity Check	LDW torque output is set to zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW torque output is 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 01-02-01	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.	C	50ms	LDW Safety block	LDW torque output is set to zero.
Technical Safety Requirement 01-02-02	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 block	LDW torque output is set to zero.
Technical Safety Requirement 01-02-03	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 block	LDW torque output is set to zero.
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	LDW torque output is set to

					zero.
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW torque output is set to zero.

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

ID	Technical Safety Requirement	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 01-01-01	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.	Max_Torque_Amplitude is the appropriate value for the upper limit of the steering torque amplitude. .	LDW functionality turns off if toque amplitude exceeds Max_Torque_Amplitude.
Technical Safety Requirement 01-01-02	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.	When LDW is deactivated, sending warning signal to the display is sufficient to inform driver.	Warning light appears on Display panel when LDW function is deactvated.
Technical Safety Requirement 01-01-03	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.	In case of failure, deactivating LDW is the safe option.	When failure occurs, LDW is deactivated.
Technical Safety Requirement 01-01-04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	Validate that data transmission checking is important as there may be cases when data transmission error can result in wrong value of LDW_Torque_Request reaching motor.	Verify that the correct (calculated)value of LDW_Torque_Request is actually received by the motor.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	Validate that memory needs to be fault free – check that accident happens when there is a fault in memory.	Verify that the memory is without any fault.
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.	Max_Torque_Frequency is the appropriate value for the upper limit of the steering torque frequency. .	LDW functionality turns off if toque frquency exceeds Max_Torque_Frequency.

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:

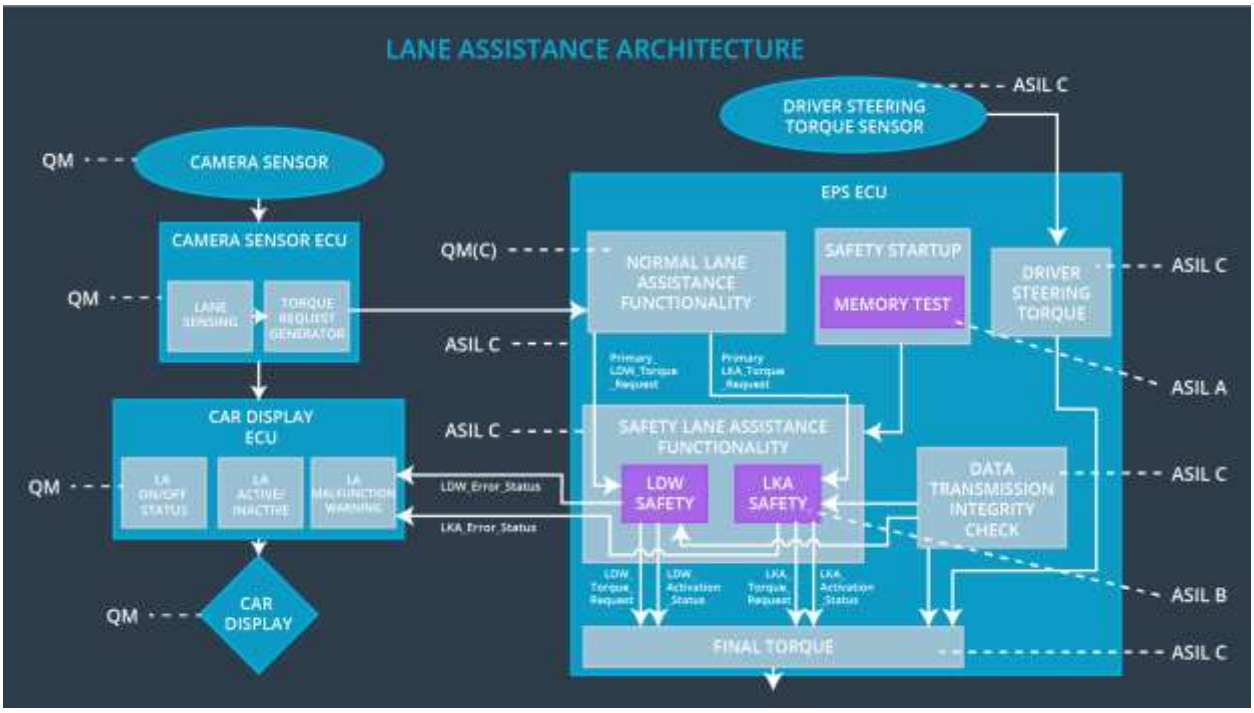
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than 'Max_Duration.	B	500ms	**LKA Safety block**	LKA torque output is set to zero.
Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	B	500ms	**LKA Safety block**	LKA torque output is set to zero.
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.	B	500ms	**LKA Safety block**	LKA torque output is set to zero.

Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity Check	LKA torque output is set to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LKA torque output is set to zero.

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

ID	Technical Safety Requirement	Validation Acceptance Criteria	Verification Acceptance Criteria
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque applied is less than 'Max_Duration.	'Max_Duration is the appropriate value for the upper limit of the torque duration for driver to not consider it as an autonomous vehicle. .	LKA functionality turns off if torque is applied for more than Max_Duration.
Technical Safety Requirement 02-01-02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.	When LKA is deactivated, sending warning signal to the display is sufficient to inform driver.	Warning light appears on Display panel when LKA function is deactivated.
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.	In case of failure, deactivating LKA is the safe option.	When failure occurs, LKA is deactivated.
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	Validate that data transmission checking is important as there may be cases when data transmission error can result in wrong value of LKA_Torque_Request reaching motor.	Verify that the correct (calculated)value of LKA_Torque_Request is actually received by the motor.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	Validate that memory needs to be fault free – check that accident happens when there is a fault in memory.	Verify that the memory is without any fault.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	EPS ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	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.	X		
Technical Safety Requirement 01-01-02	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.	X		
Technical Safety Requirement 01-01-03	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.	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	Memory test shall be conducted at start up of	X		

Safety Requirement 01-01-05	the EPS ECU to check for any faults in memory.			
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		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the LDW functionality.	LDW functionality has applied the torque of high magnitude or high frequency.	Yes	Warning on Display.
WDC-02	Turn off the LKA functionality.	LKA functionality is always on.	Yes	Warning on Display.