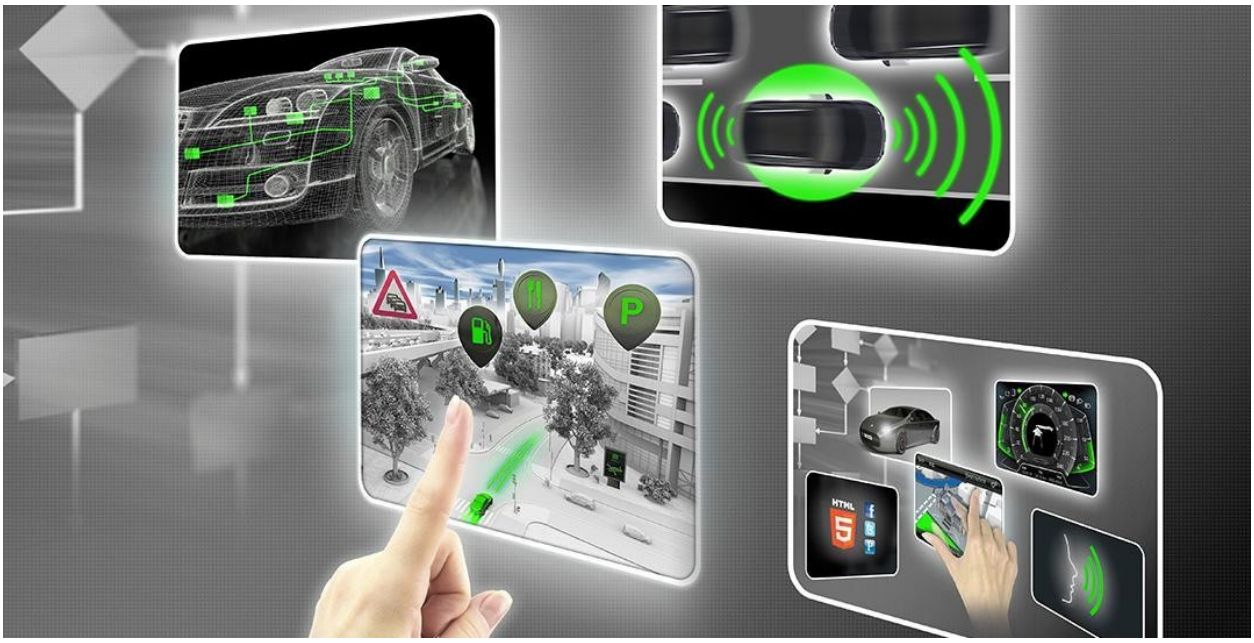
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
5/12/2018	1.0	Sara Mostafa	Intial version
6/12/2018	1.1	Sara Mostafa	Updated inputs to the Technical Safety Concept section

Table of Contents

Purpose of the Technical Safety Concept

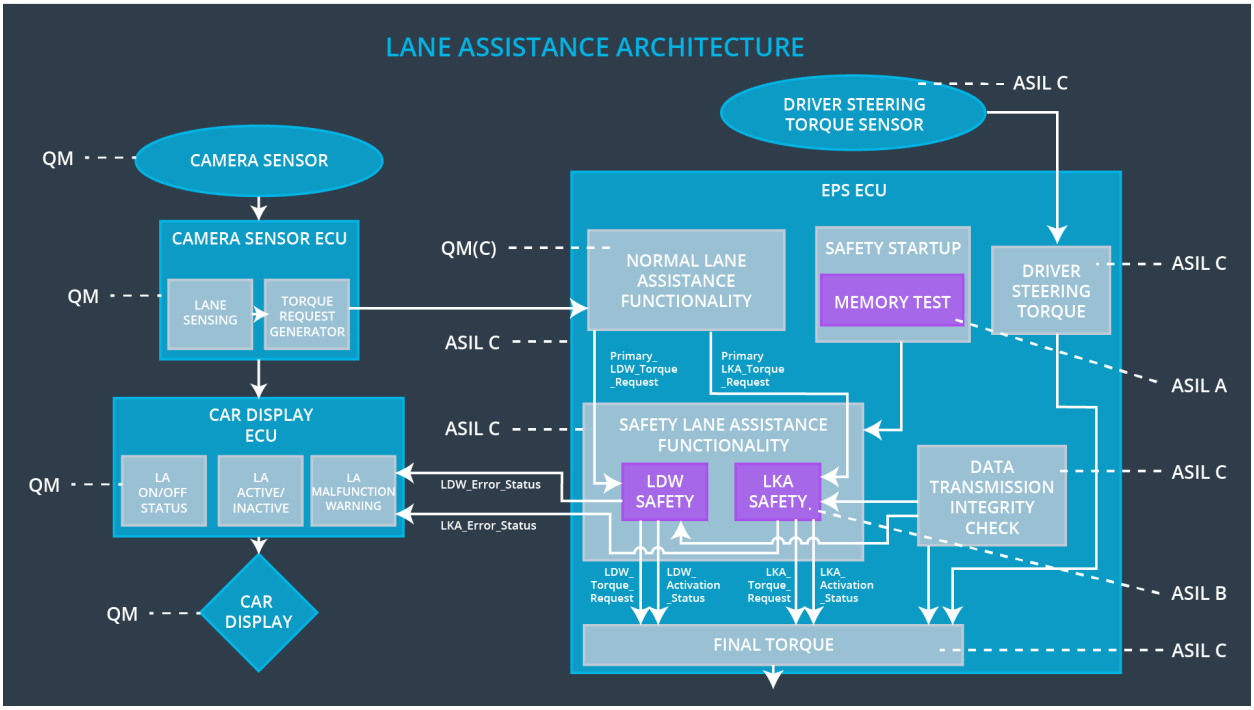
The purpose of the technical safety concept is to refine the functional safety requirements found in the functional safety concept into technical safety requirements.

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	Vibration torque amplitude below Max_Torque_Amplitude
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	Vibration torque frequency below Max_Torque_frequency
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	500	LKA Torque set to zero.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provide images to camera ECU.
Camera Sensor ECU - Lane Sensing	Detect lane lines in the images provided by camera sensor.
Camera Sensor ECU - Torque request generator	Generate Torque request to electronic power steering ECU.
Car Display	Display LKA and LDW warnings to driver.
Car Display ECU - Lane Assistance On/Off Status	Indicates that Lane assistance feature is Activated or deactivated.
Car Display ECU - Lane Assistant Active/Inactive	Indicates that Lane assistance system detect lane and is active at the moment.
Car Display ECU - Lane Assistance malfunction warning	Indicates that Lane assistance system is malfunction and fault is detected.
Driver Steering Torque Sensor	**Measure steering Torque**
Electronic Power Steering (EPS) ECU - Driver Steering Torque	analysis of driver steering torque , recieving torque request generator from camera sensor ecu and output final steering torque to Motor.
EPS ECU - Normal Lane Assistance Functionality	Recieve torque request from camera sensor and output it to safety lane assistance function.
EPS ECU - Lane Departure Warning Safety Functionality	Checks on malfunction of LDW and output final torque request.
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks on malfunction of LKA and output final torque request.
EPS ECU - Final Torque	Generate final torque recieved from LKA and LDW safety.
Motor	Responsible for providing torque to 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	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	LDW Torque to zero.
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	50 ms	LDW safety	LDW Torque to zero.
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	50 ms	LDW safety	LDW Torque 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	Data integrity	Keep last valid value.
Technical Safety Requirement 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 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	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	LDW Torque to zero.
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	50 ms	LDW safety	LDW Torque to zero.
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	50 ms	LDW safety	LDW Torque 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	Data integrity	Keep last valid value.
Technical Safety Requirement 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 to zero.

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)

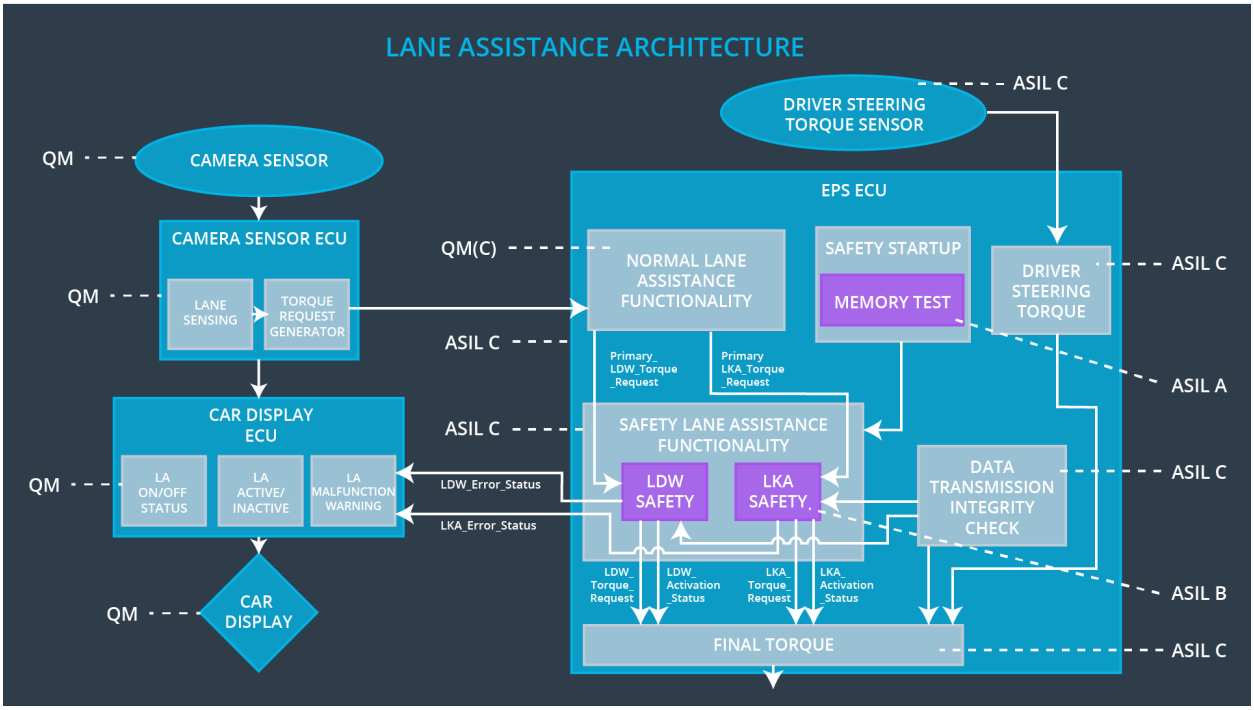
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' within Max_Duration	B	500 ms	LKA safety	LKA torque to zero.
Technical Safety Requirement 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	500 ms	LKA safety	LKA torque 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	LKA torque 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	Data integrity	Keep last valid value.
Technical Safety Requirement 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 to zero.

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

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off lane Assistant functionality	Malfunction_01	Yes	Lane Assistant Malfunction warning in the car.
WDC-02	Turn off lane Assistant functionality	Malfunction_02	Yes	Lane Assistant Malfunction warning in the car.
WDC-03	Turn off lane Assistant functionality	Malfunction_03	Yes	Lane Assistant Malfunction warning in the car.