Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0.0

Released on 2017-12-19

Document history

Date	Version	Editor	Description
19.12.2017	1.0.0	Bernhard Rode	Initial version of the safety concept

Table of Contents

Table of Contents

Purpose of the Technical Safety Concept

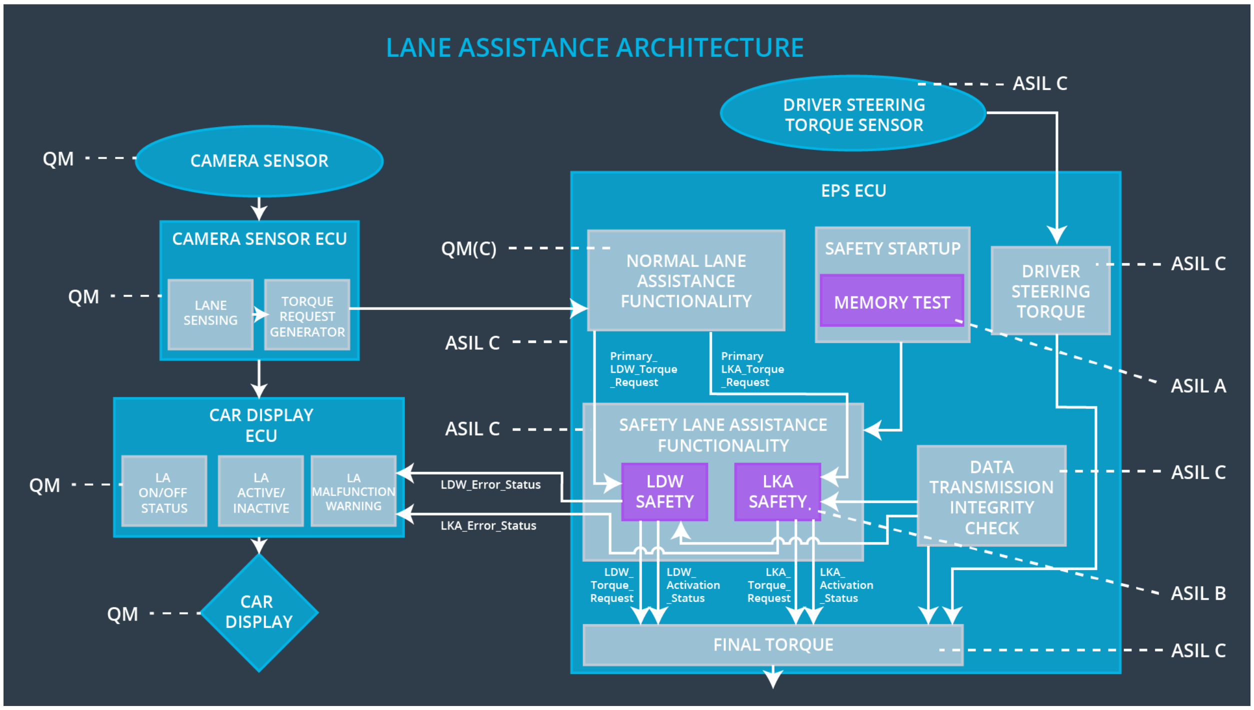
The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

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	50ms	The EPS ECU will set the oscillating torque 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	50ms	The EPS ECU will set the oscillating torque 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 EPS ECU will set the oscillating torque to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	**Description**
Camera Sensor	The camera sensor reads in images from the road
Camera Sensor ECU - Lane Sensing	Identifies when the vehicle has accidently departed its lane
Camera Sensor ECU - Torque request generator	Sends request to the electronic power steering ECU
Car Display	The car display shows messages to the driver
Car Display ECU - Lane Assistance On/Off Status	Shows the on or off status of the lane assistance function
Car Display ECU - Lane Assistant Active/Inactive	Shows the activation status of the lane assistance function
Car Display ECU - Lane Assistance malfunction warning	Shows that lane assistance function has malfunctioned
Driver Steering Torque Sensor	The driver steering torque sensor detects the steering input by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Steering input by the driver
EPS ECU - Normal Lane Assistance Functionality	Keeps the car in lane when it has accidently departed its lane
EPS ECU - Lane Departure Warning Safety Functionality	Determines when the warning messages are sent to the display
EPS ECU - Lane Keeping Assistant Safety Functionality	Determines when to activate the lane keeping assistant functionality
EPS ECU - Final Torque	The torque that is sent to the steering wheel
Motor	The steering motor provides force to 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	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 output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW torque output is set 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 output is set to zero
Technical Safety Requirement 04	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 output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Length of vehicle ignition cycle	Safety startup - 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	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 output is set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50 ms	Data Transmission Integrity Check	LDW torque output is set 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 output is set to zero
Technical Safety Requirement 04	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 output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Length of vehicle ignition cycle	Safety startup - Memory test	LDW torque output is set to zero

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:
Not needed.

Lane Keeping Assistance (LKA) Requirements:
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

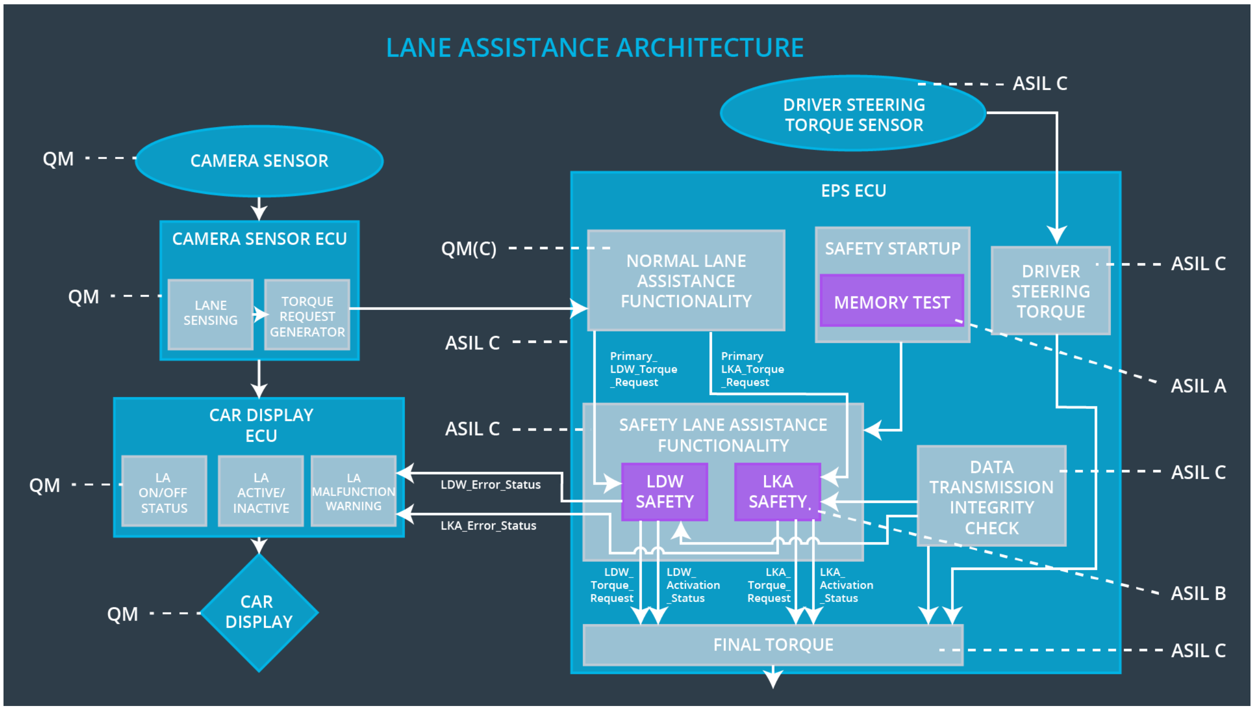
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 the duration of the torque sent to the 'Final electronic power steering Torque' component is no more than Max_Duration	B	500 ms	LKA Safety	LKA torque output 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	Data Transmission Integrity Check	LKA torque output 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	LKA torque output is set to zero
Technical Safety Requirement 04	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 output is set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	B	500 ms	Safety startup - Memory test	LKA torque output is set to zero

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:
Not needed.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, 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 the functionality	Steering torque exceeds maximum levels	Yes	Warning light on dashboard
WDC-02	turn off the functionality	Steering torque exceeds maximum levels	Yes	Warning light on dashboard