Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
10.09.2017	1.0	Sergei Dmitriev	Initial version

Abbreviation List

N	Abbreviation	Definition
1.	ASIL	Automotive Safety Integrity Level
2.	ECU	Electronic Control Unit
3.	EPS	Electronic Power Steering
4.	LA	Lane Assistance
5.	LDW	Lane Departure Warning
6.	LKA	Lane Keeping Assistance

Table of Contents

Document history 2
Abbreviation List 2
Table of Contents 2
Purpose of the Technical Safety Concept 3
Inputs to the Technical Safety Concept 3
Functional Safety Requirements 3
Refined System Architecture from Functional Safety Concept 4
Functional overview of architecture elements 4
Technical Safety Concept 5
Technical Safety Requirements 5
Refinement of the System Architecture 11
Allocation of Technical Safety Requirements to Architecture Elements 11
Warning and Degradation Concept 11

Purpose of the Technical Safety Concept

The purpose of the Technical Safety Concept is turn functional safety requirements into technical safety requirements and allocate them 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	C	50 ms	The LDW torque request shall be set 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	50 ms	The LDW torque request shall be set to zero
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the LKA torque is applied for only Max_Duration	B	500 ms	The LKA torque request shall be set to zero

Refined System Architecture from Functional Safety Concept

Refined system architecture from functional safety concept is shown in **Figure 1**.

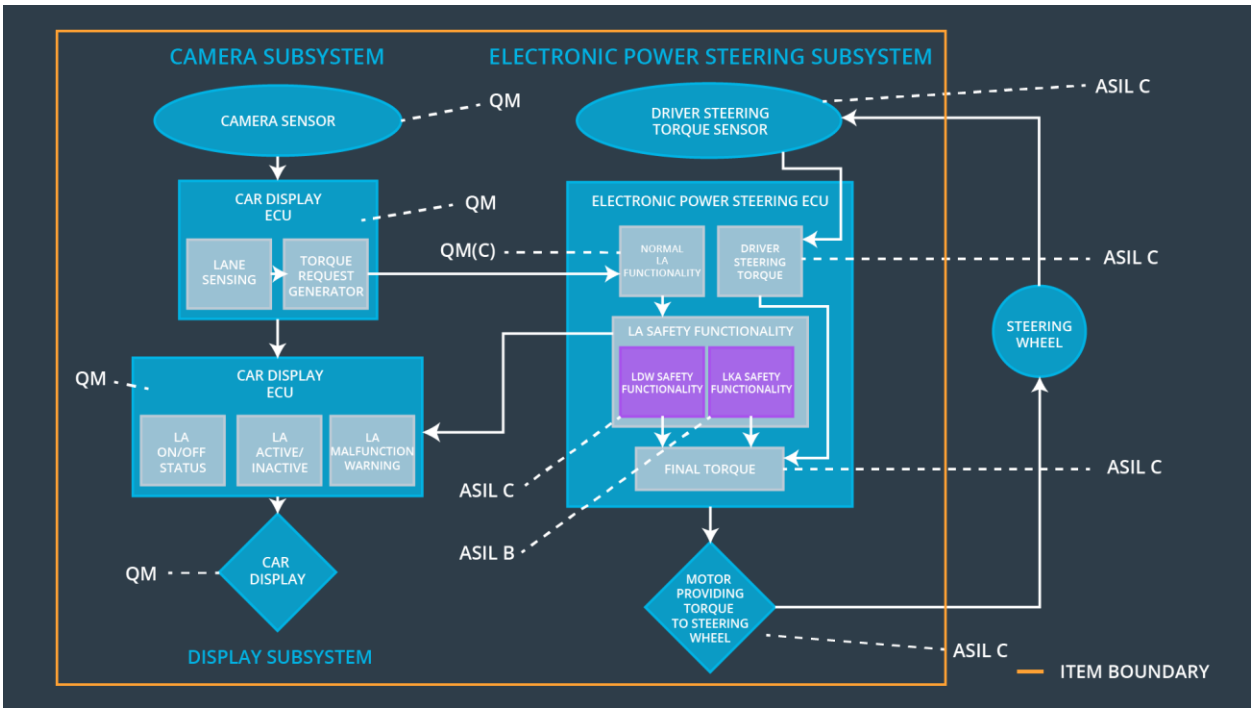

Figure 1

Functional overview of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road
Camera Sensor ECU - Lane Sensing	The Camera Sensor ECU - Lane Sensing defines lane departure
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU - Torque request generator sends torque request to EPS ECU
Car Display	The Car Display shows a driver warn signals from Camera Sensor ECU processed by the Car Display ECU
Car Display ECU - LA On/Off Status	The Car Display ECU - LA On/Off Status controls a warning light that tells the driver if the LA is on or off
Car Display ECU - LA Active/Inactive	The Car Display ECU - LA Active/Inactive controls a warning light that tells the driver if the LA is active

	or inactive
Car Display ECU - LA malfunction warning	The Car Display ECU - LA malfunction warning controls a warning light that tells the driver if the LA has a malfunction
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures steering torque provided by the driver
EPS ECU - Driver Steering Torque	The EPS ECU - Driver Steering Torque receives a signal from Driver Steering Torque Sensor, processes and sends steering torque provided by the driver to EPS ECU - Final Torque
EPS ECU - Normal LA Functionality	The EPS ECU - Normal LA Functionality processes and sends request satisfying normal functionality
EPS ECU - LDW Safety Functionality	The EPS ECU - LDW Safety Functionality processes and checks that vibrational request not above limits
EPS ECU - LKA Safety Functionality	The EPS ECU - EPS ECU - LKA Safety Functionality processes and checks that torque request not above limits
EPS ECU - Final Torque	The EPS ECU - Final Torque produces a final torque and sends it to the Motor
Motor	The Motor provide 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 01-01-01	The LDW safety component shall ensure that the amplitude of the “LDW_Torque_Request” sent to the 'EPS ECU - Final Torque' component is below Max_Torque_Amplitude	C	50 ms	LDW Safety block	LDW torque request shall be 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	50 ms	LDW Safety block	LDW torque request shall be 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” shall be set to zero	C	50 ms	LDW Safety block	LDW torque request 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	50 ms	Data Transmission Integrity Check block	LDW torque request shall be 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	Safety Startup Memory Test block	LDW torque request shall be set to zero

Functional Safety Requirement 01-02 with its associated system elements (derived in the functional safety concept):

ID	Functional Safety Requirement	Electronic Power	Camera ECU	Car Display ECU

		Steering 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 “EPS ECU - Final Torque” component is below Max_Torque_Frequency	C	50 ms	LDW Safety block	LDW torque request shall be 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	50 ms	LDW Safety block	LDW torque request shall be 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	50 ms	LDW Safety block	LDW torque request shall be 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	50 ms	Data Transmission Integrity Check block	LDW torque request shall be 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	Safety Startup Memory Test block	LDW torque request shall be set 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	Method: Testing how drivers react to different vibrational torque amplitudes set for MAX_Torque_Amplitude Acceptance Criteria: All drivers had not difficulty controlling the vehicle because the steering wheel vibration	Method: Software testing. Set vibrational torque amplitudes more than MAX_Torque_Amplitude Acceptance Criteria: The LDW torque request is set to zero within the 50 ms fault tolerant time interval
Technical Safety Requirement 01-02-01	Method: Testing how drivers react to different vibrational torque frequency set for Max_Torque_Frequency Acceptance Criteria: All drivers had not difficulty controlling the vehicle because the steering wheel vibration	Method: Software testing. Set vibrational torque frequency more than Max_Torque_Frequency Acceptance Criteria: The LDW torque request is set to zero within the 50 ms fault tolerant time interval
Technical Safety Requirement 01-01-02	Method: Testing how drivers react to the LA deactivation warning light on the car display Acceptance Criteria: The LA deactivation warning light is understandable for all drivers and it is not distract their attention	Method: Software testing. Deactivate the LDW feature Acceptance Criteria: The LDW Safety block shall send a signal to the car display ECU to turn on a warning light within the 50 ms fault tolerant time interval
Technical Safety Requirement 01-01-03	Method: Testing how drivers react to the deactivation the LDW feature Acceptance Criteria: All drivers had not difficulty controlling the vehicle during and after the deactivation the LDW feature	Method: Software testing. Simulate an error in LDW Safety block Acceptance Criteria: The LDW Safety block shall deactivate the LDW feature and the “LDW_Torque_Request” shall be set to zero within the 50 ms fault tolerant time interval

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 torque request of the “LKA_Torque_Request” sent to the 'EPS ECU - Final Torque' component is applied for only Max_Duration	B	500 ms	LKA Safety block	LKA torque request shall be 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	500 ms	LKA Safety block	LKA torque request shall be 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	500 ms	LKA Safety block	LKA torque request shall be 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	500 ms	Data Transmission Integrity Check block	LKA torque request shall be 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	Safety Startup Memory Test block	LKA torque request shall be set 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	Method: Testing how drivers react to different duration of the LKA torque request set for Max_Duration Acceptance Criteria: No drivers were dissuaded from taking their hands off the wheel	Method: Software testing. Set duration of the LKA torque request more than Max_Duration Acceptance Criteria: The LKA torque request is set to zero within the 500 ms fault tolerant time interval
Technical Safety Requirement 02-01-02	Method: Testing how drivers react to the LA deactivation warning light on the car display Acceptance Criteria: The LA deactivation warning light is understandable for all drivers and it is not distract their attention	Method: Software testing. Deactivate the LKA feature Acceptance Criteria: The LKA Safety block shall send a signal to the car display ECU to turn on a warning light within the 500 ms fault tolerant time interval
Technical Safety Requirement 02-01-03	Method: Testing how drivers react to the deactivation the LKA feature Acceptance Criteria: All drivers had not difficulty controlling the vehicle during and after the deactivation the LKA feature	Method: Software testing. Simulate an error in LKA Safety block Acceptance Criteria: The LKA Safety block shall deactivate the LKA feature and the “LKA_Torque_Request” shall be set to zero within the 500 ms fault tolerant time interval

Refinement of the System Architecture

Refined system architecture is shown in **Figure 2**.

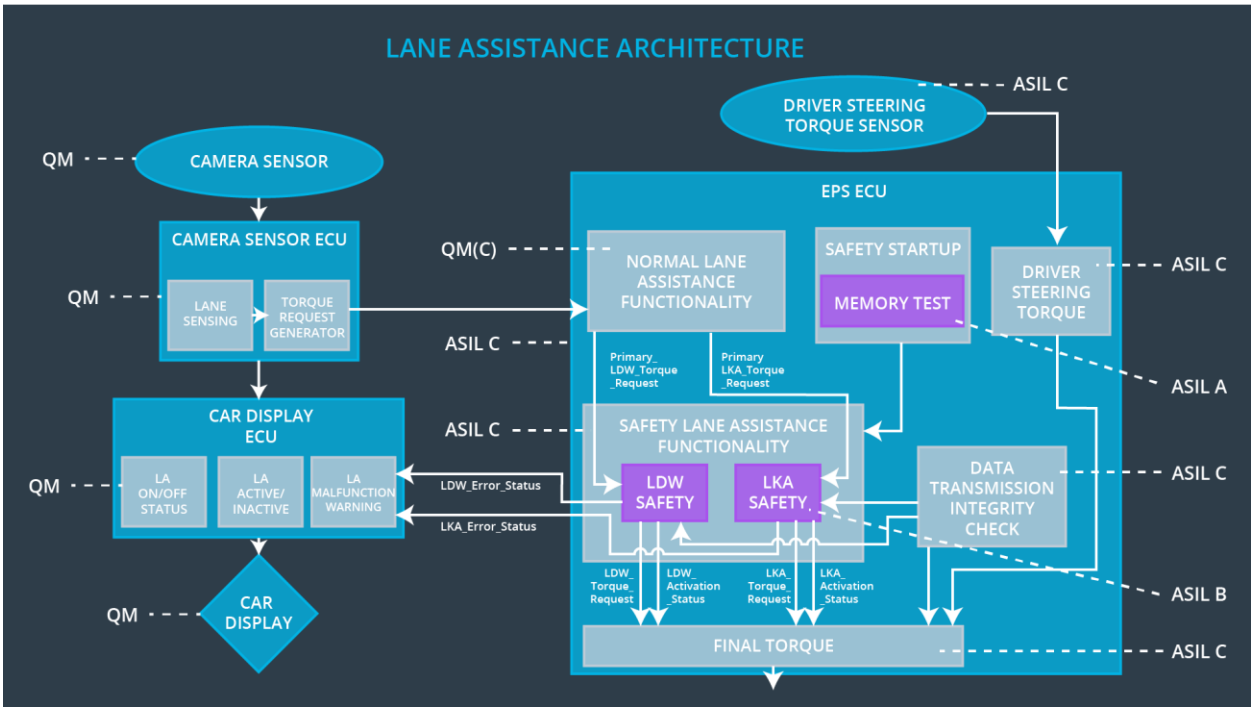

Figure 2

Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering ECU. Details in the tables above with description of technical safety requirements.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Vibrational torque request received by the Electronic Power Steering ECU is very high	Vibrational torque request is higher than MAX_Torque_Amplitude or MAX_Torque_Frequency	Yes	Display a malfunction warning light on the driver dashboard
WDC-02	Duration of the	Duration of	Yes	Display a

	LKA torque request received by the electronic power steering ECU is long	torque request is more than Max_Duration		malfunction warning light on the driver dashboard