Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 3.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-03-13	1.0	Abhishek Mantha	Document initialization
2018-03-13	2.0	Abhishek Mantha	Revising for Final Submission
2018-03-14	3.0	Abhishek Mantha	Final Submission

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 subsystem ECUs communicate with each other.

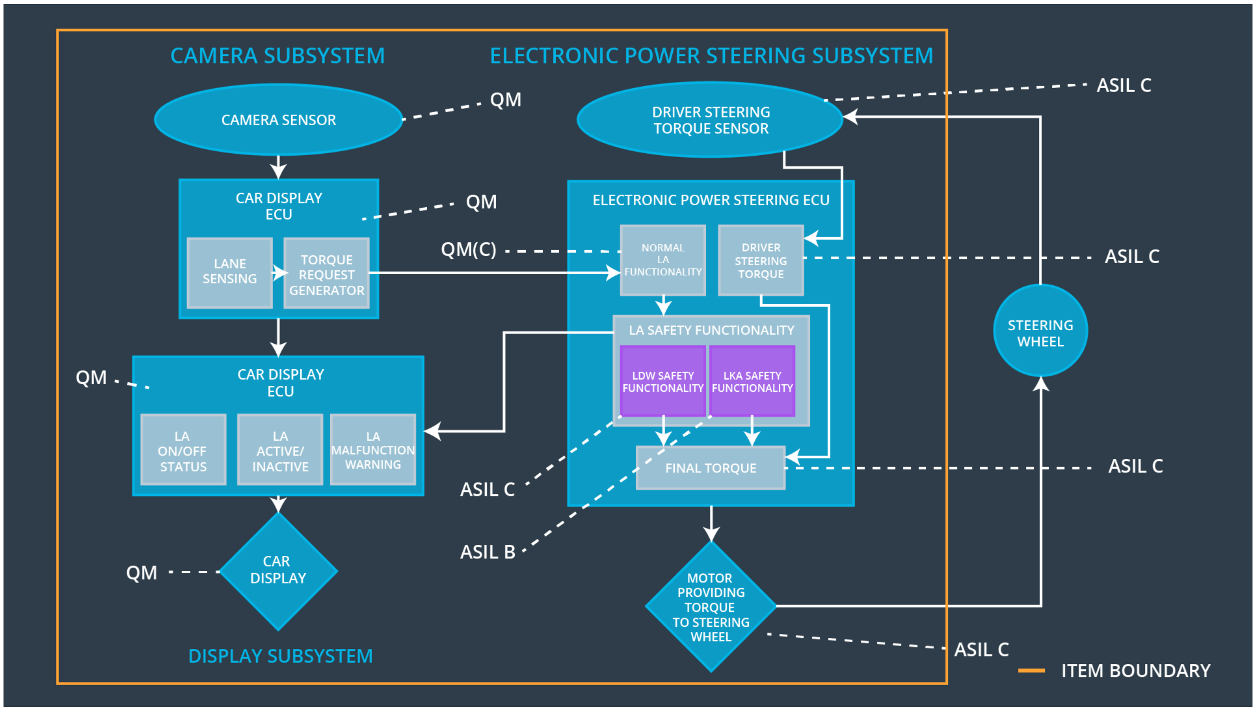
Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	A	Fault	Safe State

		SIL	Tolerant Time Interval	
Functional Safety Requirement 01-01	Electronic Power Steering ECU shall ensure that oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude	C	50 ms	LDW will set oscillating torque amplitude to 0
Functional Safety Requirement 01-02	Electronic Power Steering ECU shall ensure that oscillating torque frequency requested by LDW function is below Max_Torque_Frequency.	C	50 ms	LDW will set oscillating torque amplitude to 0
Functional Safety Requirement 02-01	Electronic Power Steering ECU shall ensure that lane keeping assistance torque requested by LKA function is applied for only Max_Duration.	C	500 ms	LKA will set oscillating torque amplitude to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Collects and transmits current camera images to Car Display ECU
Camera Sensor ECU - Lane Sensing	Determines if vehicle is correctly within bounds of current lane or if lane change maneuver is being taken w/o turn signal
Camera Sensor ECU - Torque request generator	Generates oscillating torque request applied to steering wheel if Lane Sensing component identifies that additional torque must be applied
Car Display	Displays notifications/warnings to driver dashboard
Car Display ECU - Lane Assistance On/Off Status	Determines if Lane Assistance is currently turned on and transmits appropriate display notification to Car Display
Car Display ECU - Lane Assistant Active/Inactive	Transmits appropriate display notification to Car Display if LDW or LKA functions are executed only if Lane Assistant is Active
Car Display ECU - Lane Assistance malfunction warning	Transmits malfunction warning display notification to Car Display if LDW or LKA functions are executed and Lane Assistance is On and Lane Assistant is Active
Driver Steering Torque Sensor	Collects and transmits current steering wheel torque to EPS ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Determines how much oscillating torque to apply to steering wheel based on current vehicle maneuver and on Lane Assistance Status level
EPS ECU - Normal Lane Assistance Functionality	Executes normal lane assistance functionality if vehicle departs from lane without turn signal and lane keep assistance is activated
EPS ECU - Lane Departure Warning Safety Functionality	Executes lane departure warning safety functionality and transmits appropriate signal to Car Display ECU and appropriate torque amount to apply to Final Torque component
EPS ECU - Lane Keeping Assistant Safety Functionality	Executes lane keeping assistance safety functionality and transmits appropriate signal to Car Display ECU and appropriate torque amount to apply to Final Torque component
EPS ECU - Final Torque	Determines the appropriate amount of torque to

	apply to steering wheel
Motor	Apply final 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 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	LDW safety block shall ensure that amplitude of ‘LDW_Torque_Request’ sent to EPS ‘Final Torque’ component is below ‘Max_Torque_Amplitude’.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 02	As soon as LDW function deactivates LDW feature, the 'LDW Safety' software block shall send ‘LDW_Error_Status’ to car display ECU to turn on warning light.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.

Technical Safety Requirement 03	As soon as failure is detected by LDW function, it shall deactivate LDW feature and 'LDW_Torque_Request' shall be set to 0.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 04	Validity and integrity of data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check Component	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 05	Memory test shall be conducted at start up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Component	‘LDW_Torque_Request’ shall be set to 0.

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	LDW safety component shall ensure that frequency of ‘LDW_Torque_Request’ sent to EPS ‘Final Torque’ component is below ‘Max_Torque_Frequency’.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement	As soon as LDW function deactivates LDW feature, the 'LDW Safety' software block	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set

02	shall send ‘LDW_Error_Status’ to Car Display ECU to turn on warning light.				to 0.
Technical Safety Requirement 03	As soon as failure is detected by LDW function, it shall deactivate LDW feature and 'LDW_Torque_Request' shall be set to 0.	C	50 ms	LDW Safety Functionality Block	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 04	Validity and integrity of data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check Component	‘LDW_Torque_Request’ shall be set to 0.
Technical Safety Requirement 05	Memory test shall be conducted at start up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Component	‘LDW_Torque_Request’ shall be set to 0.

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

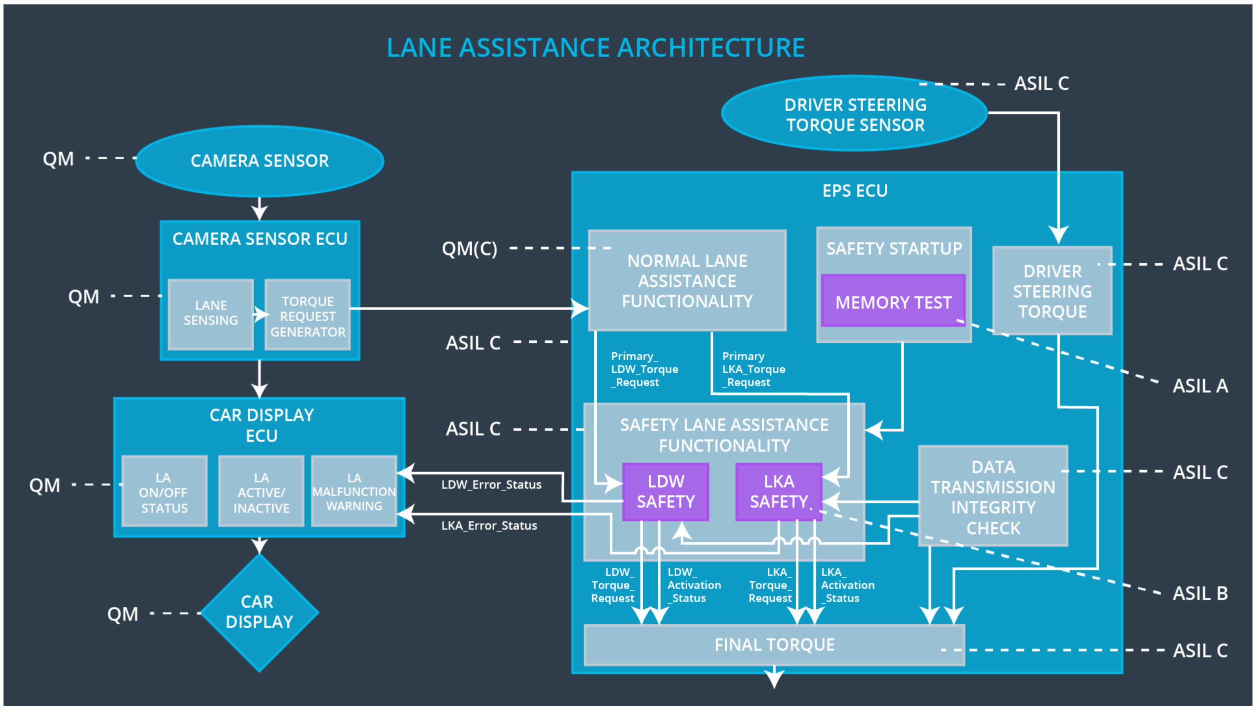
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	LKA safety component shall ensure that amplitude of ‘LKA_Torque_Request’ sent to EPS Final Torque	B	500 ms	LKA Safety Functionality Block	‘LKA_Torque_Request’ shall be set to 0.

	component is below ‘Max_Duration’.				
Technical Safety Requirement 02	As soon as LKA function deactivates LKA feature, LKA Safety software block shall send ‘LKA_Error_Status’ to Car Display ECU to turn on warning light.	B	500 ms	LKA Safety Functionality Block	‘LKA_Torque_Request’ shall be set to 0.
Technical Safety Requirement 03	As soon as failure is detected by LKA function, it shall deactivate LKA feature and LKA_Torque_Request' shall be set to 0.	B	500 ms	LKA Safety Functionality Block	‘LKA_Torque_Request’ shall be set to 0.
Technical Safety Requirement 04	Validity and integrity of data transmission for LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check Component	‘LKA_Torque_Request’ shall be set to 0.
Technical Safety Requirement 05	Memory test shall be conducted at start up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup Component	‘LKA_Torque_Request’ shall be set to 0.

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. Please refer to the above table under “Technical Safety Requirements” for a detailed specification of component architecture allocations.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW disabled; torque request will be set to 0.	The LDW warning is giving **MORE** torque than what is safe.	Yes	Warning light appears on dashboard.
WDC-02	LKA disabled; torque request will be set to 0.	The LKA function has **NO** time limit.	Yes	Warning light appears on dashboard