Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/31/2017	1.0	Me	First draft

Table of Contents

Purpose of the Technical Safety Concept

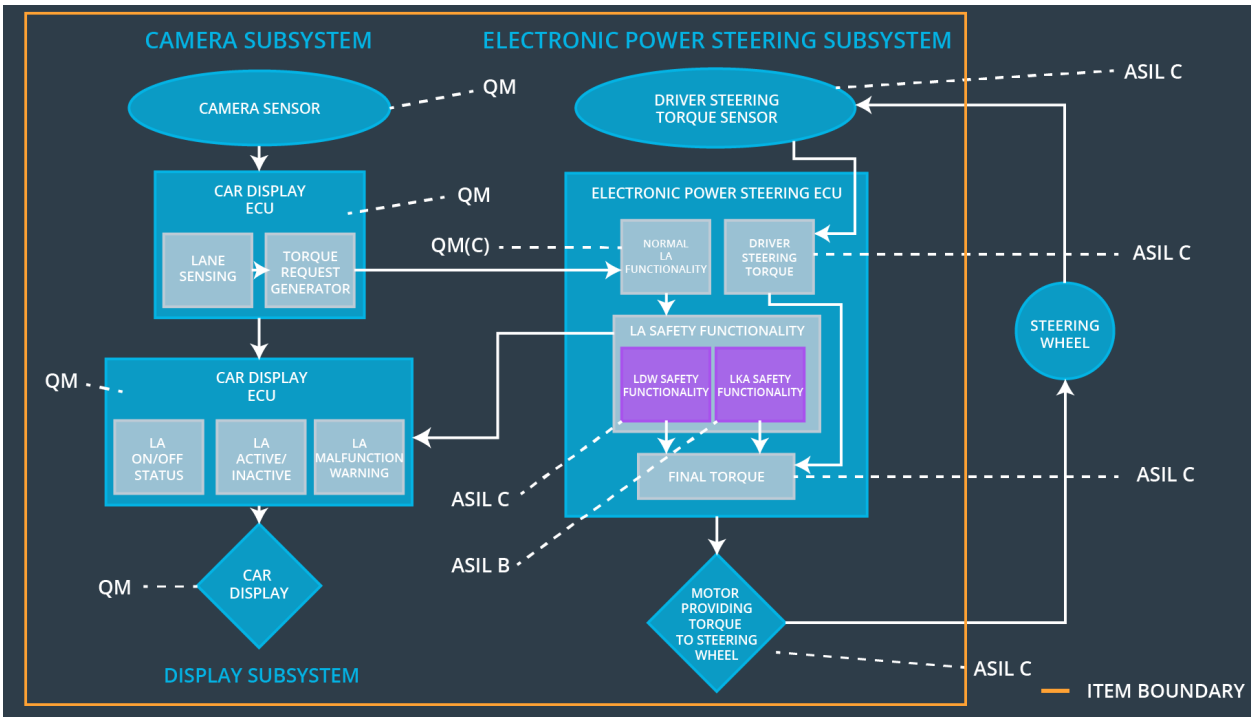
The Lane Assistance Technical Safety Concept decomposes the Lane Assistance functional requirements into technical safety requirements and allocates them to the system's architecture.

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	Torque applied by the Lane Assistance item is 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	Torque applied by the Lane Assistance item is 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	Torque applied by the Lane Assistance item is zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Collects images of the external environment and provides to Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Processes the images and determines position of vehicle with respect to the lane. Identifies lane departure
Camera Sensor ECU - Torque request generator	If lane departure conditions are met, sends request to Electronic Power Steering ECU with info about the departure
Car Display	Notifies driver of current status of Lane Assistance feature
Car Display ECU - Lane Assistance On/Off Status	Determines if Lane Assistance item is on or off and provides info to Car Display
Car Display ECU - Lane Assistant Active/Inactive	Determines if Lane Assistance item is currently active or inactive and provides to Car Display
Car Display ECU - Lane Assistance	Determines if Lane Assistance item has a

malfunction warning	malfunction and provides to Car Display
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives torque from Driver Steering Torque Sensor and determines the response (driver input torque only)
EPS ECU - Normal Lane Assistance Functionality	Receives request from Camera Sensor ECU - Torque request generator and determines the amount of torque to apply given the departure conditions
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the torque request for the LDW function meets functional safety requirements (amplitude and frequency). Outputs torque request for LDW.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the torque request for the LKA function meets functional safety requirements (max duration). Outputs torque request for LKA.
EPS ECU - Final Torque	Adds the LKA, LDW, and driver torque requests and sends to the motor.
Motor	Applies the calculated torque 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	50ms	LDW Safety	'LDW_Torque_Request' set 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	50ms	LDW Safety	'LDW_Torque_Request' 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	50ms	LDW Safety	'LDW_Torque_Request' set to zero
Technical Safety Requirement 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_Request' 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 Ignition Cycle	Safety Startup	'LDW_Torque_Request' 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	50ms	LDW Safety	'LDW_Torque_Request' set 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	50ms	LDW Safety	'LDW_Torque_Request' 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	50ms	LDW Safety	'LDW_Torque_Request' set to zero
Technical Safety Requirement 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_Request' 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 Ignition Cycle	Safety Startup	'LDW_Torque_Request' set to zero

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

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:

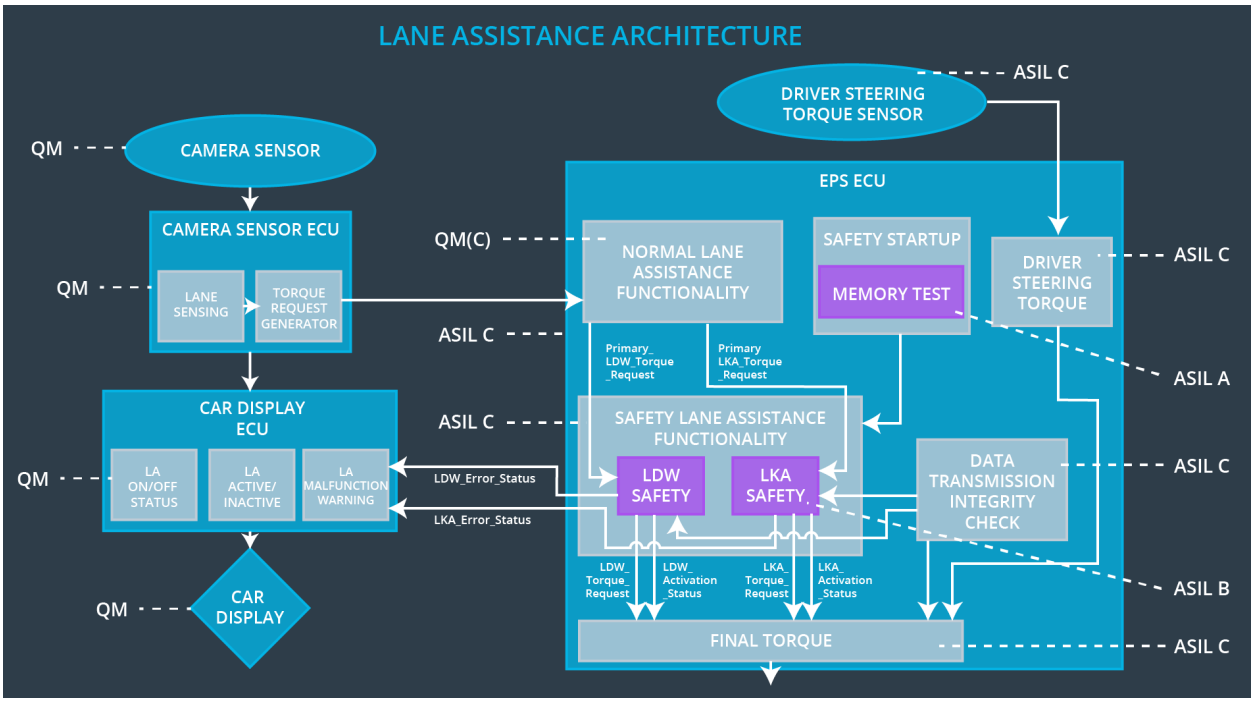
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the length of time that the 'LKA_Torque_Request' is sent to the 'Final electronic power steering Torque' component no longer than 'Max_Torque_Duration.	B	500ms	LKA Safety	'LKA_Torque_Request' set 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	500ms	LKA Safety	'LKA_Torque_Request' 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	500ms	LKA Safety	'LKA_Torque_Request' set to zero
Technical Safety Requirement 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_Request' 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 Ignition Cycle	Safety Startup	'LKA_Torque_Request' set to zero

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

As described in the Technical Safety Requirements tables, all Lane Assistance 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 Departure Warning functionality	Malfunction_01 Malfunction_02	Yes	LDW malfunction warning provided by Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	LKA malfunction warning provided by Car Display