Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
25/12/2018	V1.0	Xu YP	Version 1
25/12/2018	V1.1	Xu YP	Modify base on Version 1

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Technical Safety Concept

Technical safety concept is more concrete and gets into the details of the item's technology, and is part of the product development phase. Technical safety requirements are defined and allocated to the system
Architecture

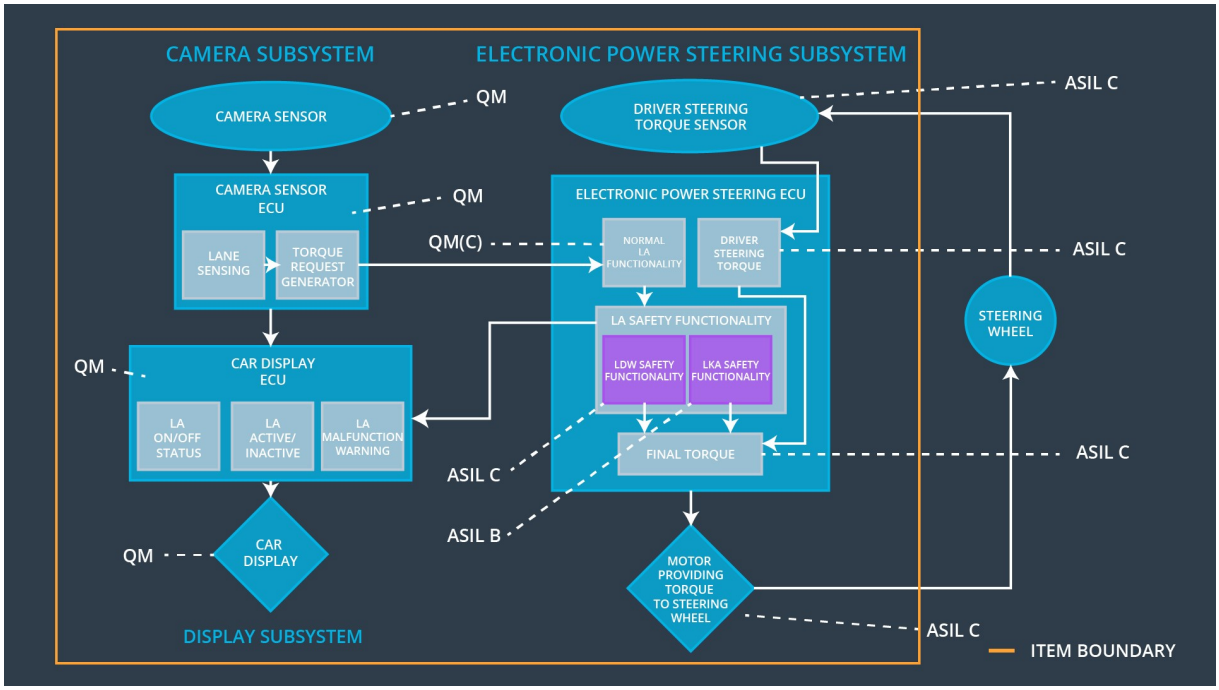
Inputs to the Technical Safety Concept

Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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 LDW oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the LDW oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Vibration 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	500ms	Lane keeping assistance torque is 0 when fault detected

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

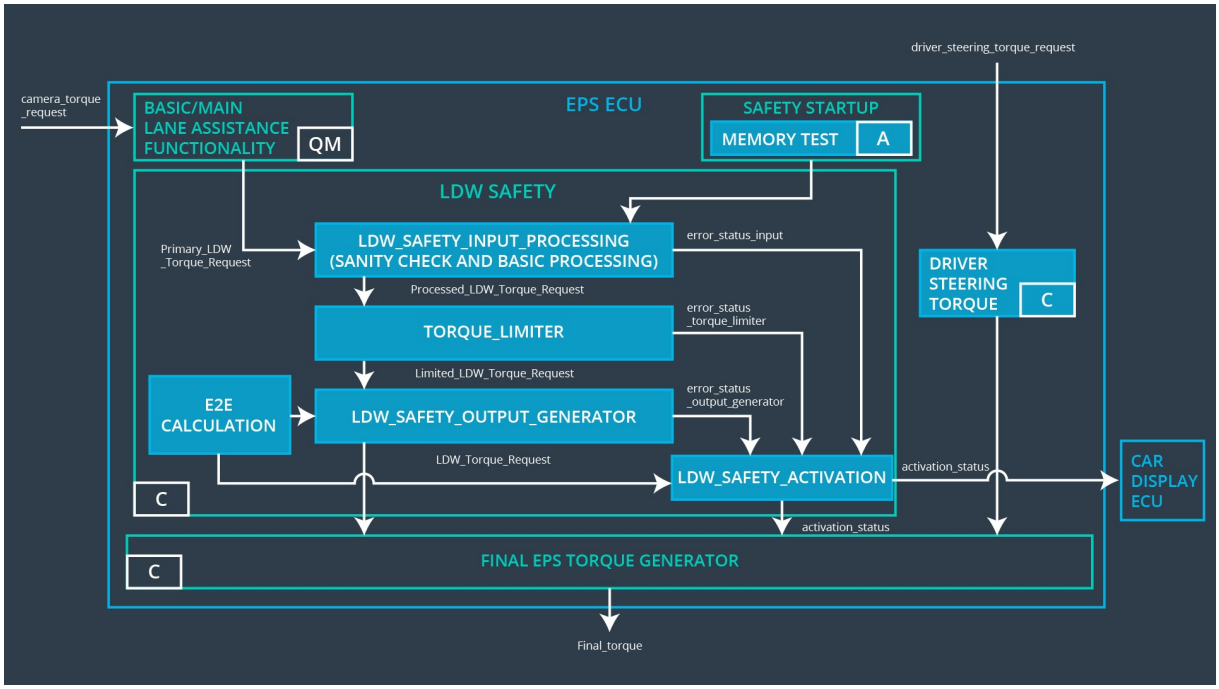
[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Capture road images and send them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detect lane line and estimate the position on the road
Camera Sensor ECU - Torque request generator	Calculating the reasonable torque to be requested to the Electronic Power Steering ECU

Car Display	Display the lane departure warning signal and the Lane Departure Assistance status.
Car Display ECU - Lane Assistance On/Off Status	Switch the signal corresponding to Lane Assistance to On/Off
Car Display ECU - Lane Assistant Active/Inactive	Decide when to activate the Lane Assistance system
Car Display ECU - Lane Assistance malfunction warning	Display the warning message of LA system malfunctioning
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Measuring the driver's steering torque.
EPS ECU - Normal Lane Assistance Functionality	Receiving the Camera Sensor ECU torque request
EPS ECU - Lane Departure Warning Safety Functionality	Limit the torque amplitude to below Max_Torque_Amplitude and torque frequency to below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Keep the car to stay in the lane within the Max_Duration time.
EPS ECU - Final Torque	Compute the final torque from the Driver Steering Torque subsystem and the Lane Assistance Safety Functionality
Motor	Actuator used to apply requested 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	50ms	LDW Safety	The LDW block set torque amplitude 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	The LDW block set torque amplitude 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	The LDW block set torque amplitude 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	The LDW block set torque amplitude 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	ignition cycle	Memory Test	The LDW block set torque amplitude 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 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	The LDW block set torque frequency 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	The LDW block set torque frequency 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_Frequency_Request' shall be set to zero	C	50ms	LDW Safety	The LDW block set torque frequency to zero.

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Frequency_Request' signal shall be ensured	C	50ms	Data Transmission Integrity Check	The LDW block set torque frequency 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	Ignition cycle	Memory Test	The LDW block set torque frequency 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		

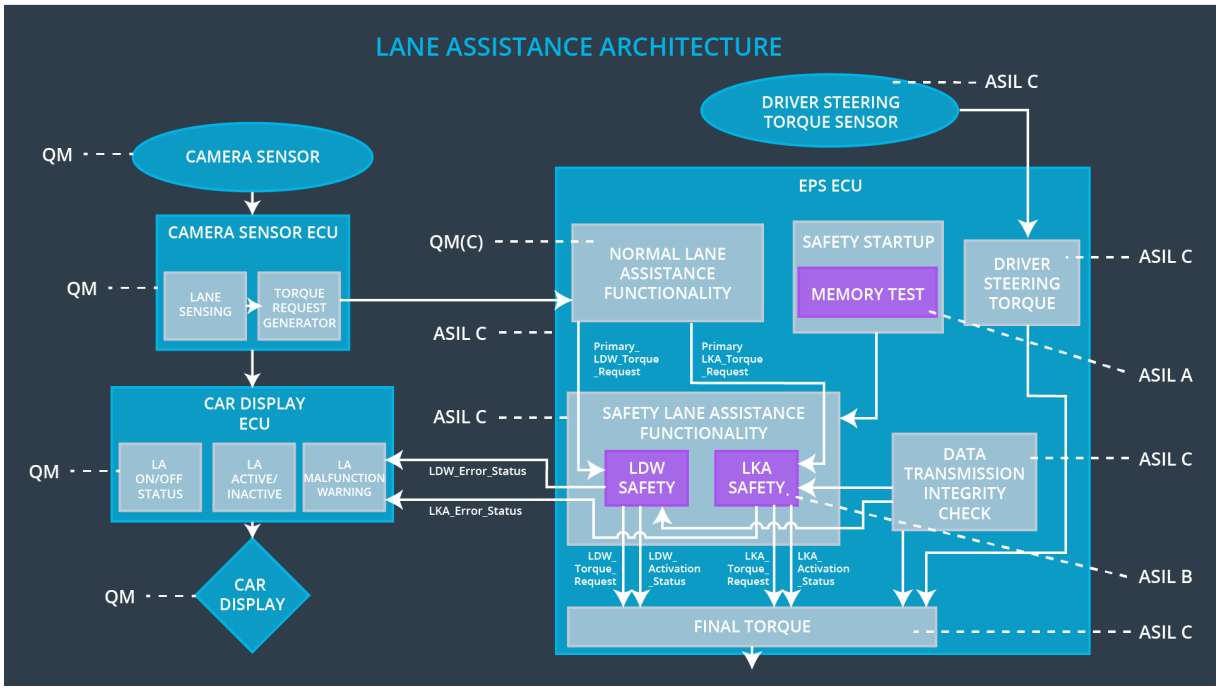
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	C	500ms	LKA Safety	Lane Keeping Assistance torque to zero
Technical Safety Requirement 02	When the LKA function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.	C	500ms	LKA Safety	Lane Keeping Assistance torque to zero
Technical Safety Requirement 03	When a failure is detected, the LKA function shall deactivate and the 'LKA_Torque_Request' shall be zero.	C	500ms	LKA Safety	Lane Keeping Assistance torque to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500ms	Data Transmission Integrity Check	Lane Keeping Assistance torque to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Memory Test	Lane Departure Warning torque 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

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	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.	X		
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.	X		
Technical Safety	As soon as a failure is detected by the LDW function, it shall	X		

Requirement 01-01-03	deactivate the LDW feature and the '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.	X		
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.	X		
Technical Safety Requirement 01-02-01	The LKA safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	X		
Technical Safety Requirement 01-02-02	When the LKA function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light.	X		
Technical Safety Requirement 01-02-03	When a failure is detected, the LKA function shall deactivate and the ‘LKA_Torque_Request’ shall be zero.	X		
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	X		
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01 Malfunction_02	Yes	Car Display the warning of LDW Malfunction
WDC-02	Turn off LKA functionality	Malfunction_03	Yes	Car Display the warning of LKA Malfunction