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
23-May-18	1	Arpit Srivastava	Version 1

Table of Contents

Purpose of the Technical Safety Concept

The purpose of a technical safety concept document is to convert the functional safety concept requirements to a more technical frame, meaning the focus is more on technical specifics rather than a bird’s eye view.

Inputs to the Technical Safety Concept

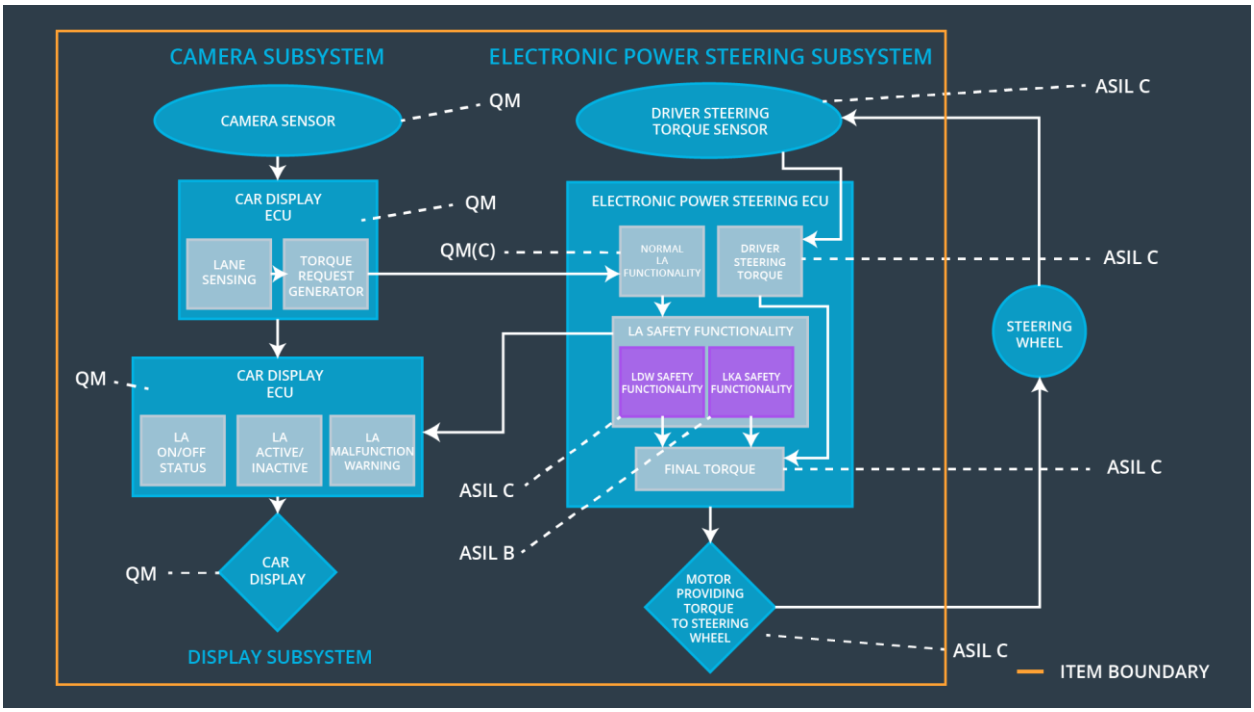
Functional Safety Requirements

[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 Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	B	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	300 ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	It will be ensured that the camera is not faulty.	C	50 ms	Input feed to lane keeping system is without lag.

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]



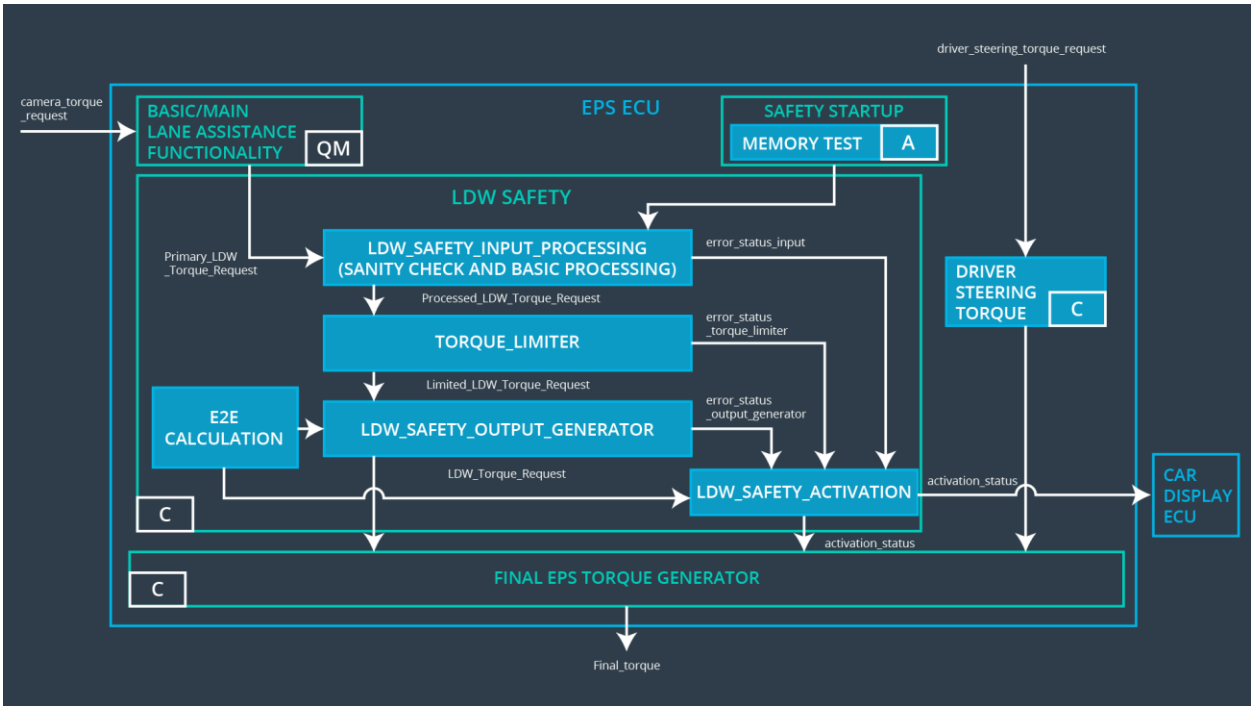
Functional overview of architecture elements

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

Element	Description
Camera Sensor	Records the camera images as a video feed of the road to provide an input to the ECU.
Camera Sensor ECU - Lane Sensing	Software module detecting the lane line positions from the Camera Sensor images.
Camera Sensor ECU - Torque request generator	Calculates the optimal torque and propagates the same.
Car Display	Display information/messages/warning for the user.
Car Display ECU - Lane Assistance	Indicate the status of the Lane Assistance

On/Off Status	functionality (On/Off.)
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the Lane Assistance functionality is properly functioning (Active/Inactive.)
Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction on the Lane Assistance functionality.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the driver's torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Software module receiving the Camera Sensor ECU torque request.
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the Lane Keeping Assistance functionality application is not active for more than Max_duration time.
EPS ECU - Final Torque	Combine the torque request from the Lane Keeping and Lane Departure Warning functionalities and sends them to the Motor.
Motor	Applies the required torque to the steering wheels.

Technical Safety Concept



Technical Safety Requirements

[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]

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	The Lane Departure Warning item shall ensure that the lane	X		

01-01	departure oscillating torque amplitude is below Max_Torque_Amplitude.			

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 Lane Departure Warning 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	Lane Departure Warning torque to zero.
Technical Safety Requirement 02	When the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 05	Memory test shall be conducted at boot up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]

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 Departure Warning 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 Lane Departure Warning 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	50 ms	LDW Safety	Lane Departure Warning torque to zero.
Technical Safety Requirement 02	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the	C	50 ms	LDW Safety	Lane Departure Warning

	Lane Departure Warning feature and set ‘LDW_Torque_Request’ to zero.				torque to zero.
Technical Safety Requirement 03	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50 ms	LDW Safety	Lane Departure Warning torque 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	The maximum torque amplitude must be validated against the lane departure system.	The lane departure system needs to be turned off.
Technical Safety Requirement 01-01-02	The ‘Torque Limiter’ is validated against the error and triggers a corresponding message to ‘LDW’ safety activator.	The warning must be displayed to the user.
Technical Safety Requirement 01-01-03	The torque request validated against zero..	The torque controller receives a .zero reading.
Technical Safety Requirement 01-01-04	Verify data transmission validity and integrity by calculating and sending the correct cyclic redundancy check (CRC) counter.	System shuts down in case of discrepancy..
Technical Safety Requirement 01-01-05	The memory test must capture memory faults.	If memory is faulty the function must turn off..
Technical Safety Requirement	The ‘Maximum Torque frequency’ must be validated against lane departure criteria.	If the torque exceeds the maximum torque the system should shut down.

01-02-01		
Requirement 01-02-02	The torque request validated against zero..	The torque controller receives a .zero reading.
Requirement 01-02-03	Verify data transmission validity and integrity by calculating and sending the correct cyclic redundancy check (CRC) counter.	System shuts down in case of discrepancy.

Lane Keeping Assistance (LKA) Requirements:

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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 Requireme	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping	C	500 ms	LKA Safety	Lane Keeping Assistance

nt 02-01-01	assistance torque is applied for less than Max_Duration				torque to zero.
Technical Safety Requirement 02-01-02	When the Lane Keeping Assistance function deactivates, the ‘LKA Safety’ shall send a signal to the Car Display ECU to turn on a warning light.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-03	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the ‘LKA_Torque_Request’ shall be zero.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	C	500 ms	LKA Safety	Lane Keeping Assistance torque to zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at boot up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	Lane Departure Warning torque to zero.

Functional Safety Requirement 02-2 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 02-2	It will be ensured that the camera is not faulty.	X		

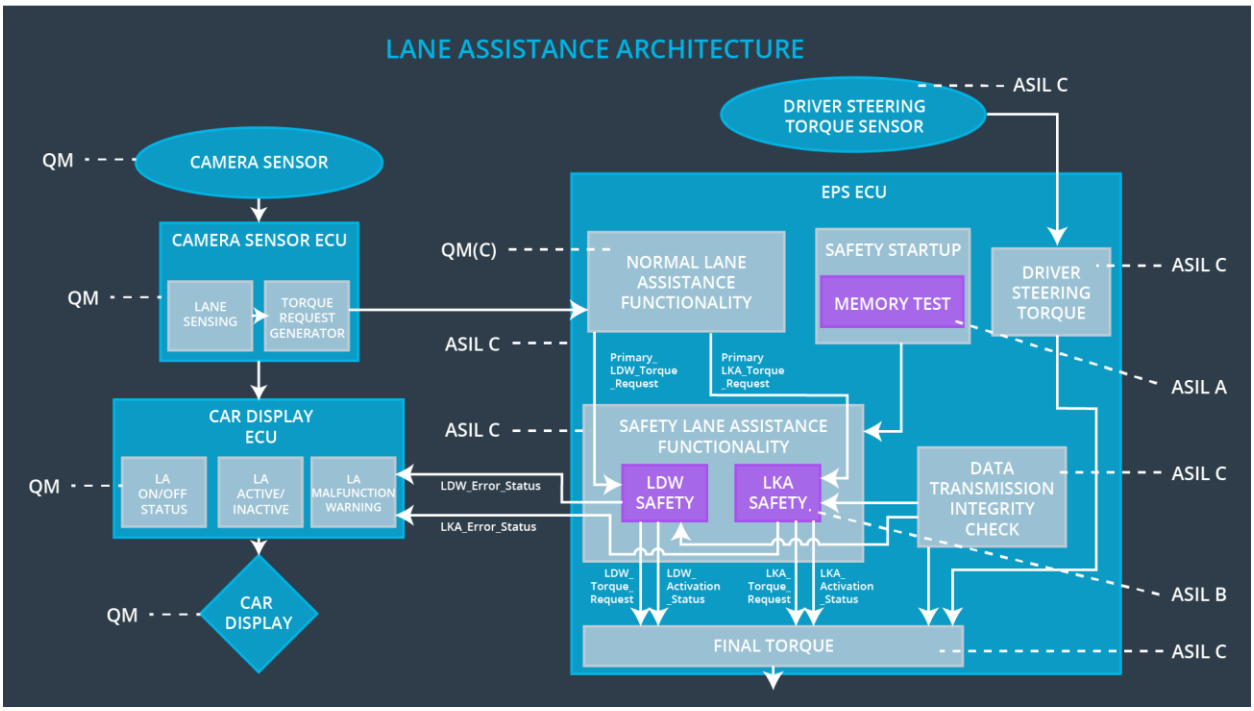
Technical Safety Requirements related to Functional Safety Requirement 02-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-02-01	The Lane Keeping Assistance safety component shall ensure the feed obtained has no lags	C	50 ms	LKA Safety	Lane Keeping assistance feed is current.
Technical Safety Requirement 02-02-02	The Lane Keeping Assistance safety component shall ensure that warning is displayed if the camera is malfunctioning.	C	500 ms	LKA Safety	Proper warning is displayed if there is a malfunction .

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-02-01	The lane keeping assistance must has no lags in real-time.	Verify the functionality is turned off if there is malfunction.
Technical Safety Requirement 02-02-02	Warning is displayed to the user.	There is a warning displayed if the function is malfunctioning and is turned off.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Technical Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Technical Safety Requirement 01-01-01	The Lane Departure Warning 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	When the Lane Departure Warning is deactivated, the ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal.	**X**		

Technical Safety Requirement 01-01-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	**X**		
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 memory problems	**X**		
Technical Safety Requirement 01-02-01	The Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	**X**		
Technical Safety Requirement 02-01-01	The Lane Keeping Assistance safety component shall ensure the duration of the lane keeping assistance torque is applied for less than Max_Duration	**X**		
Technical Safety Requirement 02-01-02	When the Lane Keeping Assistance function deactivates, the 'LKA Safety' shall send a signal to the Car Display ECU to turn on a warning light.	**X**		
Technical Safety Requirement 02-01-03	When a failure is detected, the Lane Keeping Assistance function shall deactivate and the 'LKA_Torque_Request' shall be zero.	**X**		
Technical Safety Requirement	The validity and integrity of the data transmission for	**X**		

02-01-04	‘LKA_Torque_Request’ signal shall be ensured.			
Technical Safety Requirement 02-01-05	Memory test shall be conducted at boot up of the EPS ECU to check for any memory problems	**X**		
Technical Safety Requirement 02-02-01	The Lane Keeping Assistance safety component shall ensure the feed obtained has no lags		**X**	
Technical Safety Requirement 02-02-02	The Lane Keeping Assistance safety component shall ensure that warning is displayed if the camera is malfunctioning.			**X**

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_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_02, Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display