Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
22.12.2018	1.0	Usman Ijaz Malik	First Attempt

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept

- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

Technical Safety Concept

- Technical Safety Requirements
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements

Warning and Degradation Concept

Purpose of the Technical Safety Concept

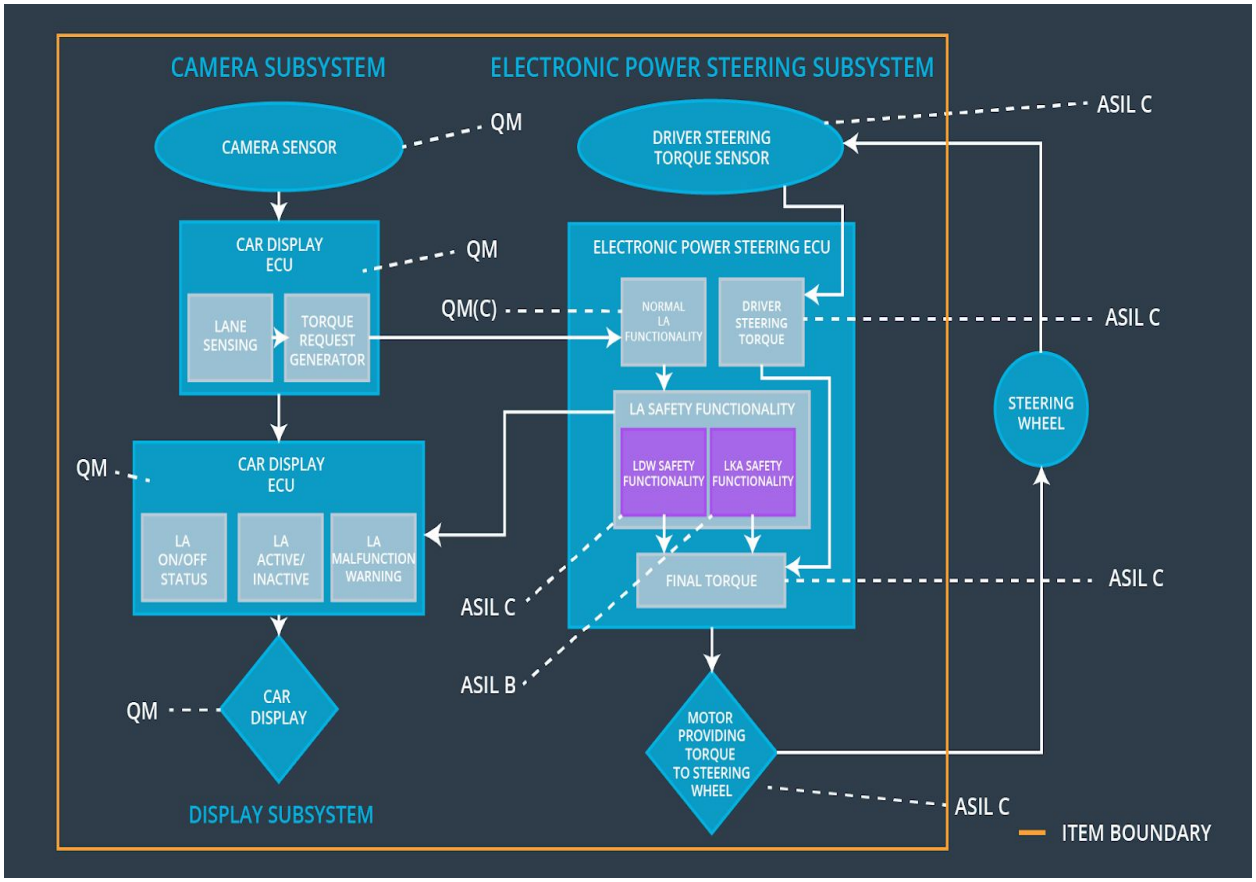
Purpose of the technical safety concept is to turn the functional safety requirements into technical safety requirements and allocating technical safety requirements to the system architecture.

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	50ms	Turn the system off after fault tolerant time interval
Functional Safety Requirement 01-02	The Lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Turn the system off after fault tolerant time interval
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	Turn the system off after fault tolerant time interval

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Capture the road images and provide it to camera sensor ECU.
Camera Sensor ECU - Lane Sensing	Detect the lanes in the images provided by the camera sensor and check for lane departures.
Camera Sensor ECU - Torque	Calculate the necessary torque which is to be

request generator	requested to EPS ECU. It also tells the car display ECU to display warning.
Car Display	It displays the warning for the driver.
Car Display ECU - Lane Assistance On/Off Status	Shows the status of Lane Assistance functionality.
Car Display ECU - Lane Assistant Active/Inactive	Shows if the lane assistance functionality is properly working or not.
Car Display ECU - Lane Assistance malfunction warning	Shows the warning related to lane assistance malfunction
Driver Steering Torque Sensor	Measure the torque applied on the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receives the torque request applied by the driver using steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Receives the camera sensor ECU torque request
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the torque amplitude is below Max_Torque_Amplitude and the torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the lane keeping assistant functionality is not applied after the Max_Duration_Time.
EPS ECU - Final Torque	Combines the torque request from the LKA and LDW functionalities and send the final torque to motor.
Motor	Applies the requested Final Torque.

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 Electric Power Steering Torque” component is below	C	50ms	Lane Departure Warning Safety	Set amplitude of the LDW_Torque_Request to zero.

	“Max_Torque_Amplitude”				
Technical Safety Requirement 02	The ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal, as soon as the LDW is deactivated.	C	50ms	Lane Departure Warning Safety	Set amplitude of the LDW_Torque_Request to zero.
Technical Safety Requirement 03	LDW function shall deactivate the the LDW feature and ‘LDW_torque_request’ shall be set to zero, as soon as a failure is detected in LDW function.	C	50ms	Lane Departure Warning Safety	Set amplitude of the LDW_Torque_Request to zero.
Technical Safety Requirement 04	Validity and Integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50ms	Data transmission integrity check	Set amplitude of the LDW_Torque_Request to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any memory fault.	A	Ignition cycle	Safety Startup	Set amplitude of the LDW_Torque_Request 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	The lane keeping item shall	X		

Safety Requirement 01-02	ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency			

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 Electric Power Steering Torque” component is below “Max_Torque_Frequency”	C	50ms	Lane Departure Warning Safety	Set frequency of the LDW_Torque_Request to zero.
Technical Safety Requirement 02	The ‘LDW Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal, as soon as the LDW is deactivated.	C	50ms	Lane Departure Warning Safety	Set frequency of the LDW_Torque_Request to zero.
Technical Safety Requirement 03	LDW function shall deactivate the the LDW feature and ‘LDW_Torque_Request’ shall be set to zero, as soon as a failure is detected in LDW function.	C	50ms	Lane Departure Warning Safety	Set frequency of the LDW_Torque_

					Request to zero.
Technical Safety Requirement 04	Validity and Integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data transmission integrity check	Set frequency of the LDW_Torque_Request to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any memory fault.	A	Ignition cycle	Safety Startup	Set frequency of the LDW_Torque_Request to zero.

Lane Keeping Assistance (LKA) Requirements:

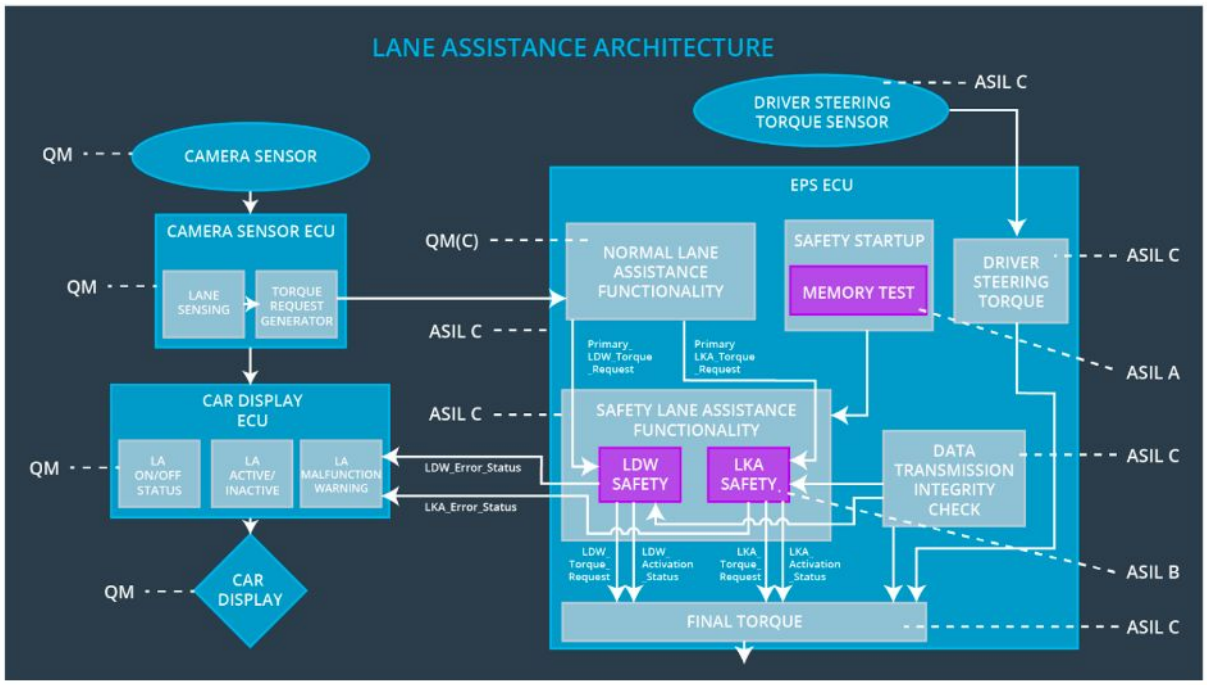
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

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	Lane Keeping Assistance safety component shall ensure that the Duration of the ‘LKA_Duration_Request’ sent to the “Final Electric Power Steering Torque” component is below “Max_Duration”	B	500ms	Lane Keeping Assistance Safety	Set Duration to zero.
Technical Safety Requirement 02	The ‘LKA Safety’ software module shall send a signal to the Car Display ECU to turn on a warning signal, as soon as the LKA feature is deactivated.	B	500ms	Lane Keeping Assistance Safety	Set Duration to zero.
Technical Safety Requirement 03	LKA function shall deactivate the the LKA feature and ‘LKA_Duration_Request’ shall be set to zero, as soon as a failure is detected in LKA function.		500ms	Lane Keeping Assistance Safety	Set Duration to zero.
Technical Safety Requirement 04	Validity and Integrity of the data transmission for ‘LKA_Duration_Request’ signal shall be ensured.	B	500ms	Data transmission integrity check	Set Duration to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the startup of EPS ECU to check for any memory fault.	A	Ignition cycle	Safety Startup	Set Duration to zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements defined above are allocated to Electronic Power Steering ECU

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the function	Malfunction_01 ,Malfunction_02	Yes	the driver will see a warning light on the dashboard when the system

				malfunctions.
WDC-02	Turn off the function	Malfunction_03	Yes	Manual would include a warning that the lane assistance system should not be used as an autonomous driving system and the driver maintains the responsibility of the safe operations of the vehicle