



Elektrobit



UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0
Released on 2018-06-15



Document history

Date	Version	Editor	Description
09-Jun-2018	0.1	Nikhil Patel	Initial Draft
13-Jun-2018	1.0	Nikhil Patel	First attempt
15-Jun-2018	2.0	Nikhil Patel	Included Udacity Reviewer Feedback

Table of Contents

Contents

Document history	2
Table of Contents.....	2
Purpose of the Technical Safety Concept	3
Inputs to the Technical Safety Concept.....	3
Functional Safety Requirements.....	3
Refined System Architecture from Functional Safety Concept.....	4
Functional overview of architecture elements.....	4
Technical Safety Concept	6
Technical Safety Requirements	6
Refinement of the System Architecture.....	11
Allocation of Technical Safety Requirements to Architecture Elements	11
Warning and Degradation Concept.....	11

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to refine the functional safety requirements established in the functional safety concept into technical safety requirement. As per the ISO 26262 standards the functional safety concept is in the concept phase while the technical safety concept is part of the product development phase. This is because the technical safety concept is more concrete and gets into the details of the item's technology. The product development phase also includes designing hardware and software. In the V model, the technical safety concept would belong to the product development at the systems level:

The technical safety concept involves:

- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

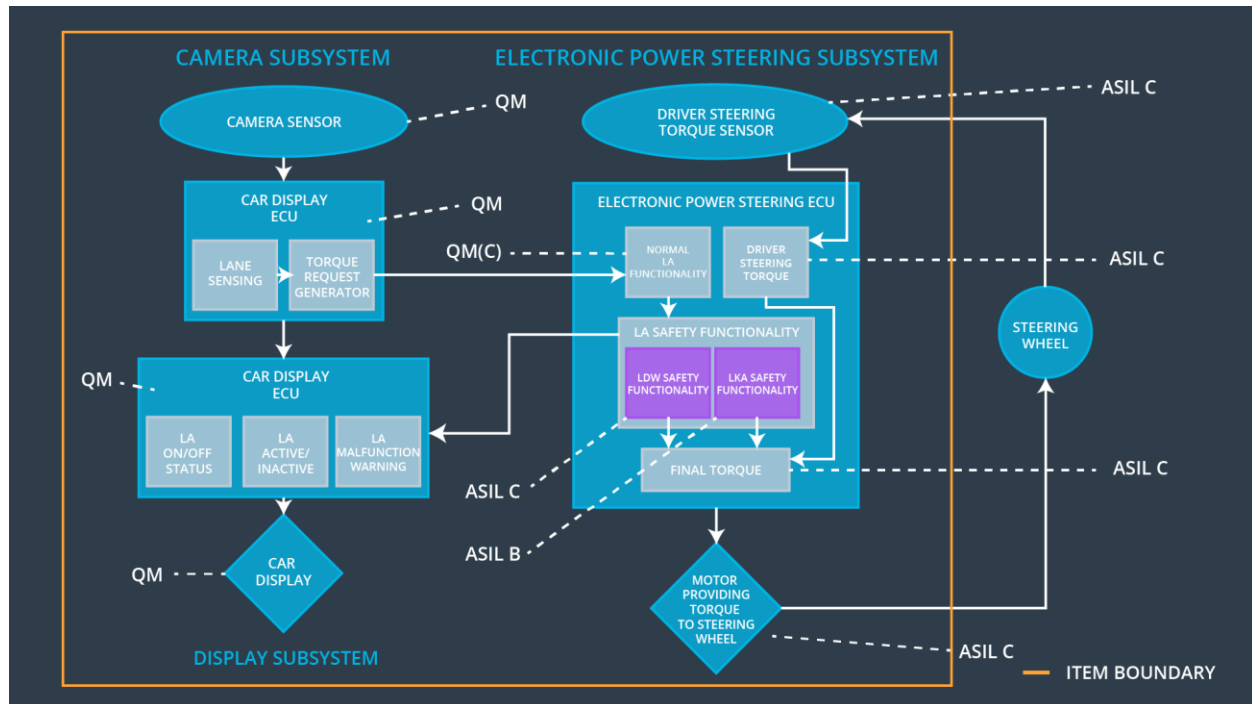
Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item should ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude value.	C	50 ms	Turn Off System
Functional Safety Requirement 01-02	The lane keeping item should ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency value.	C	50 ms	Turn Off System
Functional Safety Requirement 02-01	The electronic power steering ECU should ensure that the lane keeping assistance torque is applied for only Max_Duration value.	B	500 ms	Turn Off System
Functional Safety	The electronic power steering ECU should be deactivated when the electronic power	B	50 ms	Turn Off System

Requirement 02-02	steering ECU detects the camera sensor is not responding.			
-------------------	---	--	--	--

Refined System Architecture from Functional Safety Concept

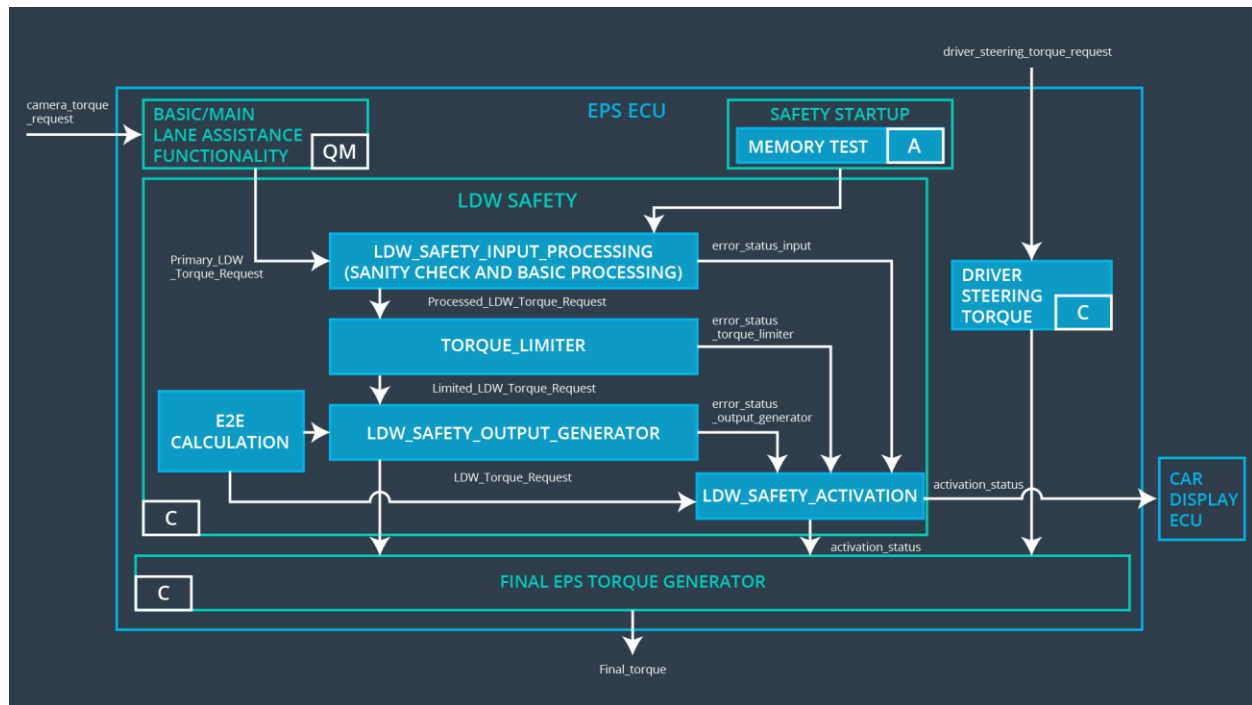


Functional overview of architecture elements

Element	Description
Camera Sensor	This Sensor responsible for capturing road images that is in- front of the vehicle pathway and provide them to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	The camera sensor ECU as a Software module inside it which is responsible for detecting the lane line positions from the input provided by the Camera Sensor images.
Camera Sensor ECU - Torque request	Software module inside camera sensor ECU

generator	responsible for calculating additional torque for LKA and LDW function. This calculated torque will be requested to EPS ECU, which would then be applied to the syste
Car Display	Car Display is responsible for providing feedback to the driver about the status of lane assistant system, thus keeping the driver updated.
Car Display ECU - Lane Assistance On/Off Status	Software module responsible for displaying On/Off status of LDW & LKA functions, thus telling the driver which module is not working and thus the driver need to take the manual control of the vehicle as in when required.
Car Display ECU - Lane Assistant Active/Inactive	Software module responsible for displaying Active/Inactive status of LDW & LKA function, thus keeping the driver updated.
Car Display ECU - Lane Assistance malfunction warning	Software module responsible for displaying warning of malfunctions in LDW & LKA function, thus keeping the driver updated.
Driver Steering Torque Sensor	Sensor responsible for measuring the torque applied on steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module responsible for process data received from Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Software module responsible for receiving torque request from Camera Sensor ECU and transfers to Safety Lane Assistance Functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the torque amplitude is below Max_Torque_Amplitude value and torque frequency is below Max_Torque_Frequency value.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module in EPS ECU responsible for ensuring that LKA is not activate more than Max_duration time and if camera sensor is failed, then LKA will be deactivated.
EPS ECU - Final Torque	Combine the torque request from the LKA safety and LDW safety functionalities and sends them to the Motor.
Motor	An electric motor that applies the torque indicated by the Electronic Power Steering ECU 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 01-01-01	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.	C	50 ms	LDW safety block	LDW_Torque_Output is set to zero
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	C	50 ms	LDW safety block	LDW_Torque_Output is set to zero
Technical Safety Requirement 01-01-03	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	50 ms	LDW safety block	LDW_Torque_Output is 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.	C	50 ms	Data Transmission Integrity Check	LDW_Activation_Status is zero
Technical Safety Requirement 01-01-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LDW_Activation_Status is zero

Functional Safety Requirement 01-02 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 <i>frequency</i> of 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency'.	C	50 ms	LDW Safety	LDW_Activation_Status is zero
Technical Safety Requirement 02	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	50 ms	LDW Safety	LDW_Activation_Status is zero
Technical Safety Requirement 03	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	50 ms	LDW Safety	LDW_Error_Status is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LDW_Activation_Status is zero

Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory.	A	ignition cycle	Memory Test	LDW_Activation_Status is zero
---------------------------------	---	---	----------------	-------------	-------------------------------

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-01 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 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 02-01-01	The LKA safety component should ensure that the amplitude of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	C	50 ms	LKA safety block	LKA_Torque_Output is set to zero
Technical Safety Requirement 02-01-02	As and when the LKA function deactivates the LKA feature, the 'LKA Safety' software block would send a signal to the car display ECU to turn on a warning light	C	50 ms	LKA safety block	LKA_Torque_Output is set to zero
Technical Safety Requirement	As and when a failure is detected by the LKA function, it should deactivate the LKA feature and	C	50 ms	LKA safety block	LKA_Torque_Output is set to zero

02-01-03	the 'LKA_Torque_Request' would be set to zero.				
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal would be ensured.	C	50 ms	Data Transmission Integrity Check	LKA_Activation_Status is zero
Technical Safety Requirement 02-01-05	Memory test should be conducted at startup of the EPS ECU to check for any type of fault in memory.	A	Ignition cycle	Memory Test	LKA_Activation_Status is zero

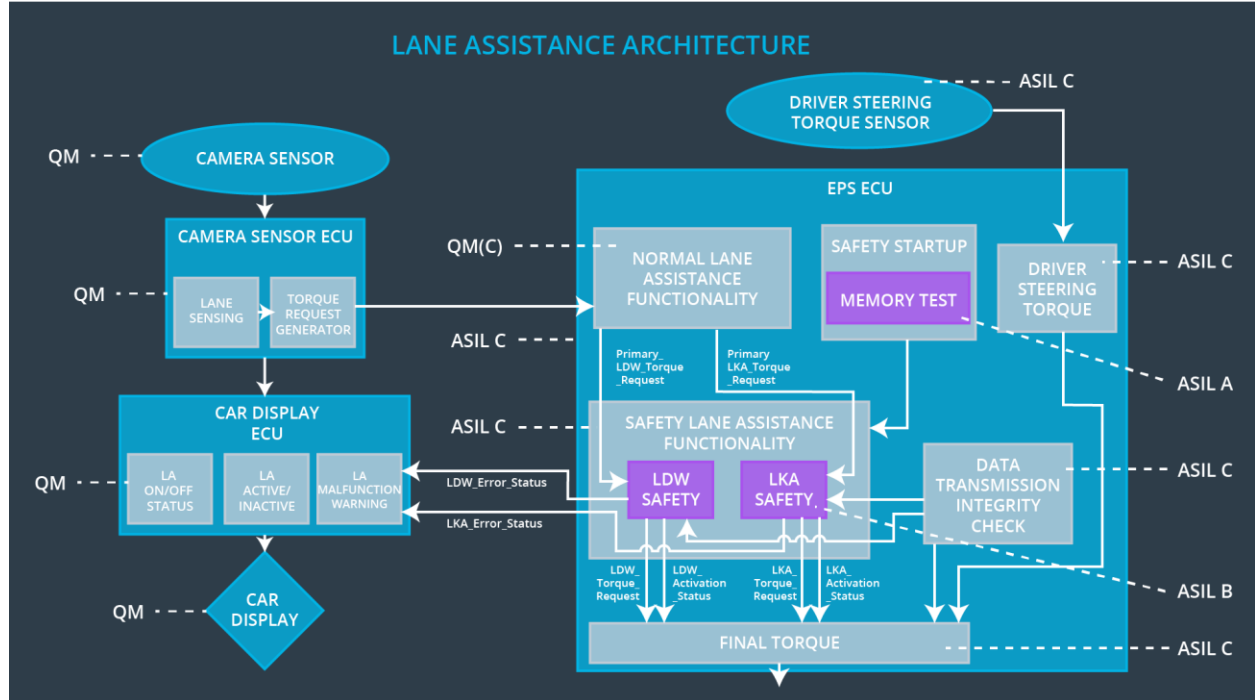
Functional Safety Requirement 02-02 with its associated system elements
(Derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-02	The electronic power steering ECU would be deactivated when the electronic power steering ECU detects the camera sensor is not working.	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	As and when a failure is detected by the Camera Sensor, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	C	50 ms	LKA safety block	LKA_Activation_Status is zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For the Lane Assistance item, all technical safety requirements are allocated to the Electronic Power Steering ECU. For the exact allocation within EPS ECU, please refer to the technical safety requirements tables above.

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	Turn on warning light of the LDW functionality
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_04	Yes	Turn on warning light of the LKA functionality