Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
26-05-2018	0.1	Harveen Singh	Initial Draft
27-05-2018	1.0	Harveen Singh	Finalized Version

Table of Contents

Purpose of the Technical Safety Concept

The Technical Safety Concept defines how the subsystems interact at message level and describes how the ECU's communicate with each other. Technical safety concept is part of the product development phase. The product development phase also includes designing hardware and software.

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	50 ms	Set Lane Departure Warning Torque Request Amplitude to zero.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Set Lane Departure Warning Torque Request Frequency to zero.
Functional Safety Requirement 02-01	Lane keeping assistance Function will be time limited for a Max_Duration	B	500ms	Set Lane Keeping Assistance torque to zero and shut off the system

Refined System Architecture from Functional Safety Concept

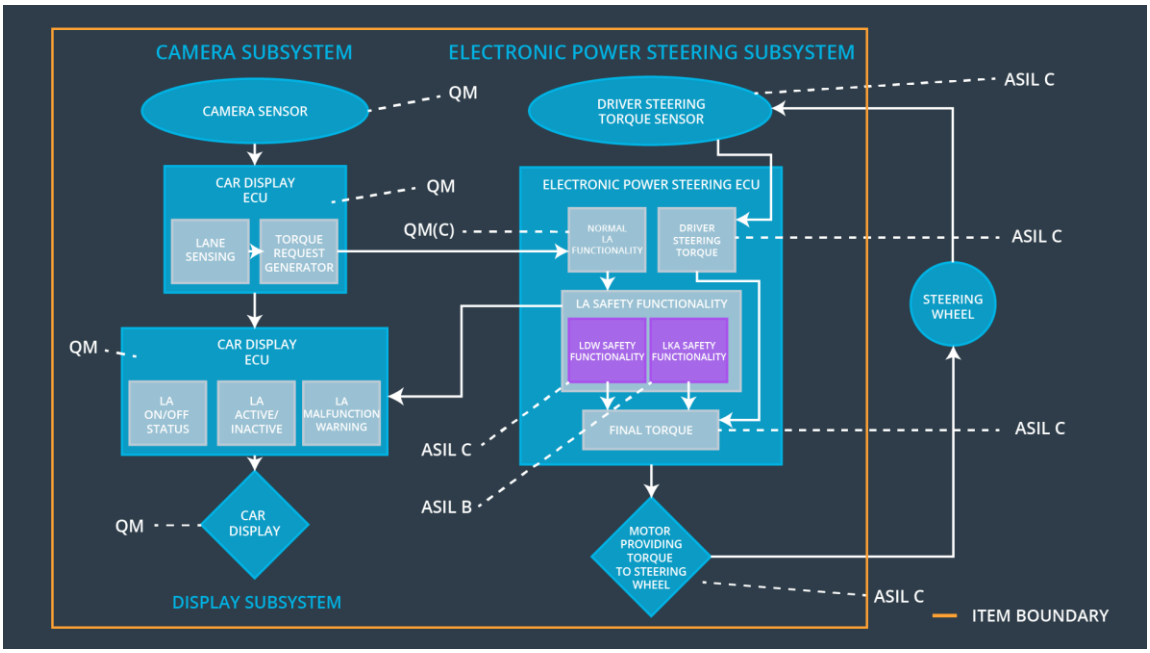

Fig 1. Lane Assistance System Architecture
[image source Udacity course content]

Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images and send to camera ECU
Camera Sensor ECU - Lane Sensing	Senses the lanes and sends output to torque request generator in case car leaves the lane.
Camera Sensor ECU - Torque request generator	Generate torque request to Electronic Power Steering ECU
Car Display	Display status and warnings of the system
Car Display ECU - Lane Assistance On/Off Status	Displays whether the lane assistance system is turned on or off.
Car Display ECU - Lane Assistant Active/Inactive	Displays whether the Lane Assistance system is active or inactive.
Car Display ECU - Lane Assistance malfunction warning	Displays any malfunction or warnings in the Lane Assistance system
Driver Steering Torque Sensor	measures torque applied to the steering wheel.

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes input from Driver Steering Torque sensor.
EPS ECU - Normal Lane Assistance Functionality	It takes input from Driver Steering Torque Sensor and camera ECU and passes it to the safety lane assistance functionality
EPS ECU - Lane Departure Warning Safety Functionality	Checks for any malfunction in the Lane Departure Warning function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn't any malfunction)
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks for any malfunction in the Lane Keeping Assistance function and take appropriate action. (deactivate if there is malfunction, pass the output torque to the final torque is there isn't any malfunction)
EPS ECU - Final Torque	Combine the inputs from LDW , LKA safety functionality and driver steering torque to deliver the final torque request to the motor
Motor	Provides 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	As soon as the 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	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature , '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	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 03	Memory test shall be conducted at startup of the EPS ECU to check for any FAULTS in memory	A	The length of ignition cycle	Data Transmission Integrity Check	Lane Departure Warning Torque Request Amplitude shall be set 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 block	Lane Departure Warning Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 05	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	Lane Departure Warning Torque Request Amplitude shall be 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	As soon as the 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	Lane Departure Warning Torque Request Frequency shall be set to zero.
Technical Safety Requirement 02	As soon as the LDW function deactivates the LDW feature , ‘LDW safety’ software block shall send a signal to the car	C	50 ms	LDW Safety block	Lane Departure Warning Torque Request Frequency shall be set to zero

	display ECU to turn on a warning light				
Technical Safety Requirement 03	Memory test shall be conducted at startup of the EPS ECU to check for any FAULTS in memory	A	The length of ignition cycle	Data Transmission Integrity Check	Lane Departure Warning Torque Request Frequency shall be set 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 block	Lane Departure Warning Torque Request Frequency shall be set to zero
Technical Safety Requirement 05	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_Frequency.	C	50 ms	LDW Safety block	Lane Departure Warning Torque Request Frequency shall be set 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	As soon as the failure is detected by the LKA function , it shall deactivate the LKA feature and the ‘LKA_Torque_Request’ shall be set to zero	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request shall be set to zero
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature , ‘LKA safety’ software block shall send a signal to the car display ECU to turn on a warning light	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request shall be set to zero
Technical Safety Requirement 03	Memory test shall be conducted at startup of the EPS ECU to check for any FAULTS in memory	A	The length of ignition cycle	Data Transmission Integrity Check	Lane Keeping Assistance Torque Request shall be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured.	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request shall be set to zero
Technical Safety Requirement 05	The LKA safety component shall ensure that duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration’.	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request shall be set to zero

Refinement of the System Architecture

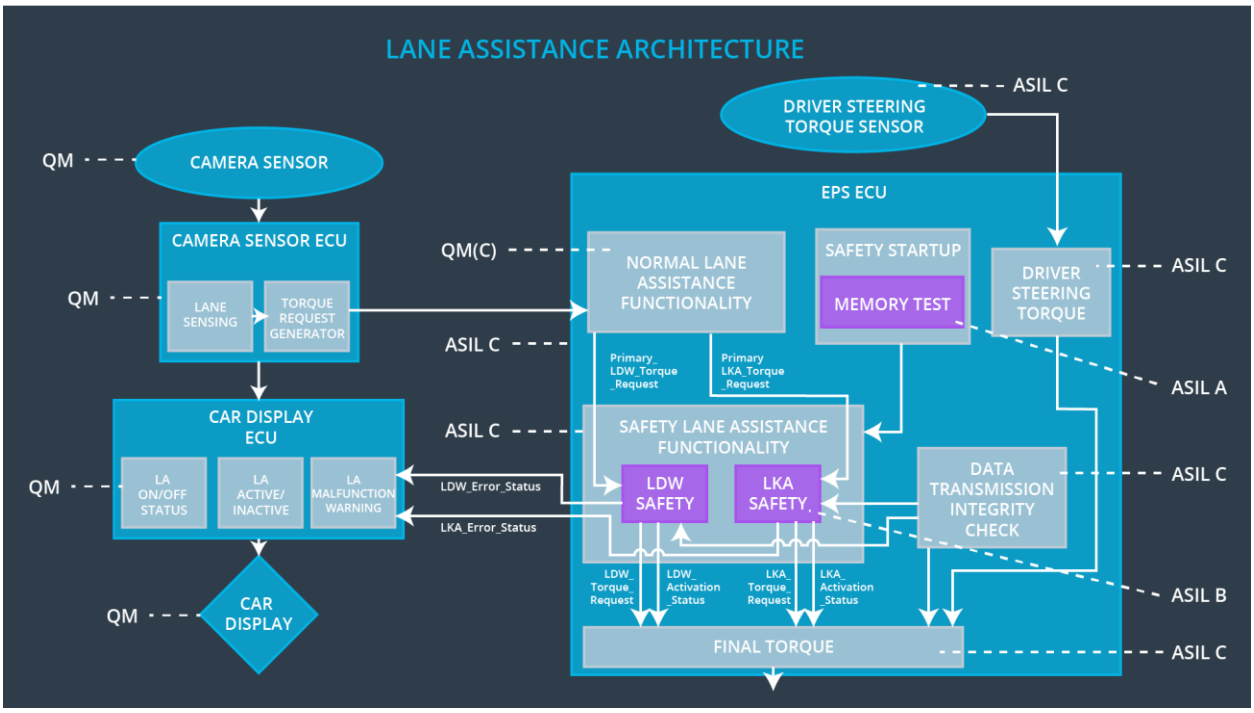

Fig 2. Refined Lane Assistance System Architecture
[image source Udacity course content]

Allocation of Technical Safety Requirements to Architecture Elements

All The Technical Safety Requirements like LDW (Lane Departure Warning) Safety, LKA (Lane Keeping Assistance) Safety and memory are assigned to the EPS ECU (Fig. 2)

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn OFF the Functionality	Malfunction_01 Malfunction_02	Yes	Warning Light on Dashboard and warnings displayed on car display
WDC-02	Turn OFF the Functionality	Malfunction_03	Yes	Warning Light on Dashboard and warnings displayed on car display