Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-02-02	1.0	Greg Yeutter	Initial Draft
2018-02-05	2.0	Greg Yeutter	LKA Safe State Modification

Table of Contents

Purpose of the Technical Safety Concept

The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

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 warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW will set the oscillating torque amplitude to 0.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Frequency	C	50 ms	LDW will set the oscillating torque amplitude to 0.
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	500 ms	LKA will set the oscillating torque amplitude to 0.

Refined System Architecture from Functional Safety Concept

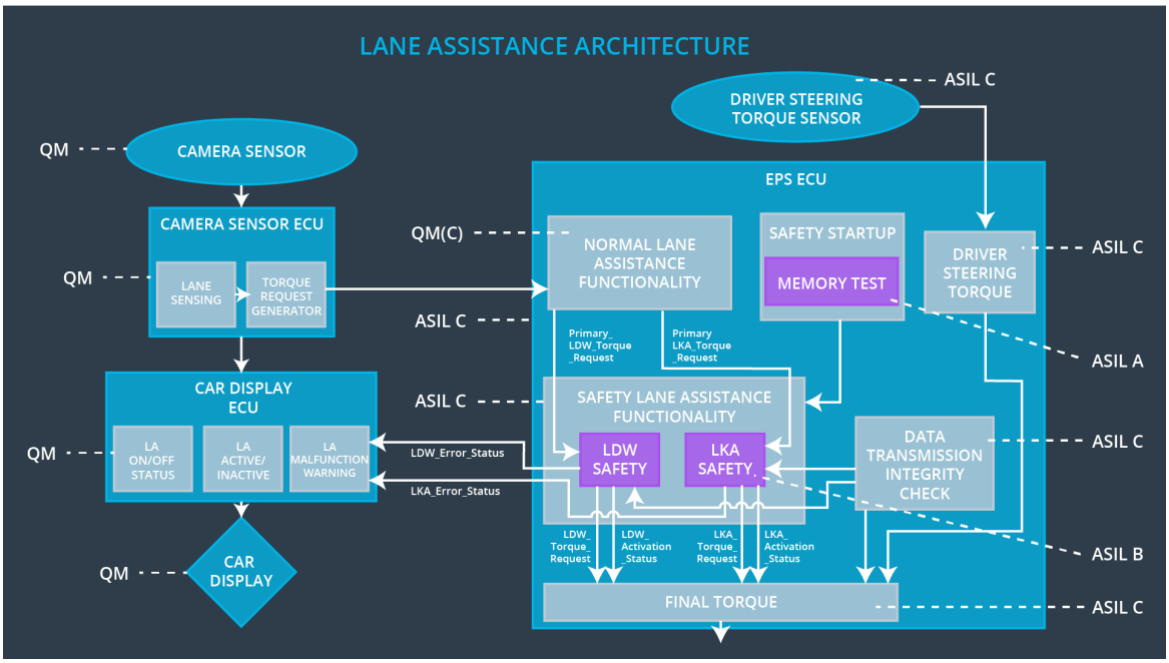

Figure 1: System Architecture Diagram

Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images of the road surface and sends the images to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Receives input from the Camera Sensor. Identifies when the vehicle has accidentally departed the ego lane and sends the appropriate signal to the Torque request generator of the Camera Sensor ECU.
Camera Sensor ECU - Torque request generator	When the Lane Sensing block of the Camera Sensor ECU detects a lane departure, the torque request generator sends a signal to the Electronic Power Steering ECU to apply steering torque to correct the position.
Car Display	Displays warnings generated by the Car Display

	ECU to the driver about the status of various subsystems.
Car Display ECU - Lane Assistance On/Off Status	Displays the on/off status of the Lane Assistance system.
Car Display ECU - Lane Assistant Active/Inactive	Displays the active or inactive status of the Lane Assistance system.
Car Display ECU - Lane Assistance malfunction warning	Turns on when the Lane Assistance system malfunctions.
Driver Steering Torque Sensor	Senses the amplitude and frequency of steering torque and sends the information to the Electronic Power Steering ECU.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Determines the current amount of torque applied in the steering system.
EPS ECU - Normal Lane Assistance Functionality	Receives torque requests from the Camera Sensor ECU and passes relevant torque requests to the LDW and LKA blocks.
EPS ECU - Lane Departure Warning Safety Functionality	Activates when there is a Primary_LDW_Torque_Request, generating a torque request to the Final Torque block.
EPS ECU - Lane Keeping Assistant Safety Functionality	Activates when there is a Primary_LKA_Torque_Request, generating a torque request to the Final Torque block.
EPS ECU - Final Torque	Combines torque requests from the LDW Safety block and LKA safety block with the driver steering torque to a final output torque.
Motor	Applies the steering torque defined by the Final Torque block.

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	50 ms	LDW Safety	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50 ms	Data Transmission Integrity Check	Lane Departure Warning Torque Request Amplitude shall be set 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	50 ms	LDW Safety	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical Safety Requirement 04	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	Lane Departure Warning Torque Request Amplitude shall be set 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	Length of vehicle ignition cycle	Memory Test	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	The LDW safety component shall ensure that 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 Request Frequency shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50 ms	Data Transmission Integrity Check	Lane Departure Warning Torque Request Frequency shall be set 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	50 ms	LDW Safety	Lane Departure Warning Torque Request Frequency shall be set to zero
Technical Safety Requirement 04	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	Lane Departure Warning Torque Request Frequency shall be set 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	Length of vehicle ignition cycle	Memory Test	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	The LKA safety component shall ensure that the amplitude of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is set to zero once 'Max_Duration' has been exceeded	B	500 ms	LKA Safety	Lane Keeping Assistance Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured	B	500 ms	Data Transmission Integrity Check	Lane Keeping Assistance Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 03	As soon as a 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	Lane Keeping Assistance Torque Request Amplitude shall be set to zero.
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display	B	500 ms	LKA Safety	Lane Keeping Assistance Torque Request Amplitude shall be set to zero.

	ECU to turn on a warning light				
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Length of vehicle ignition cycle	Memory Test	Lane Keeping Assistance Torque Request Amplitude shall be set to zero.

Refinement of the System Architecture

Refer to Figure 2 for the System Architecture Diagram.

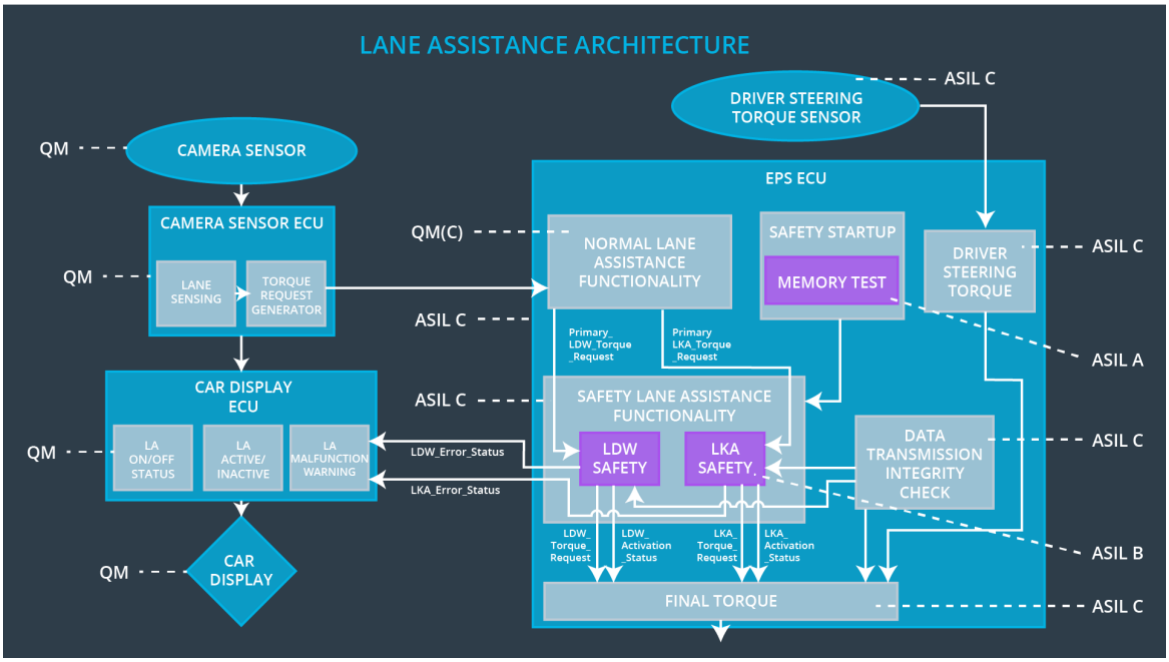

Figure 2: System Architecture Diagram

Allocation of Technical Safety Requirements to Architecture Elements

For the item outlined in this document, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Steering torque frequency and/or amplitude are degraded.	Steering torque exceeds Max_Torque_Frequency and/or Max_Torque_Amplitude	Yes	Warning light on dashboard.
WDC-02	Lane keeping assistance function will turn off.	Torque is applied for a duration exceeding Max_Duration	Yes	Warning light on dashboard.