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
28-10-18	1.0	Madhukar	First Draft

Table of Contents

Purpose of the Technical Safety Concept

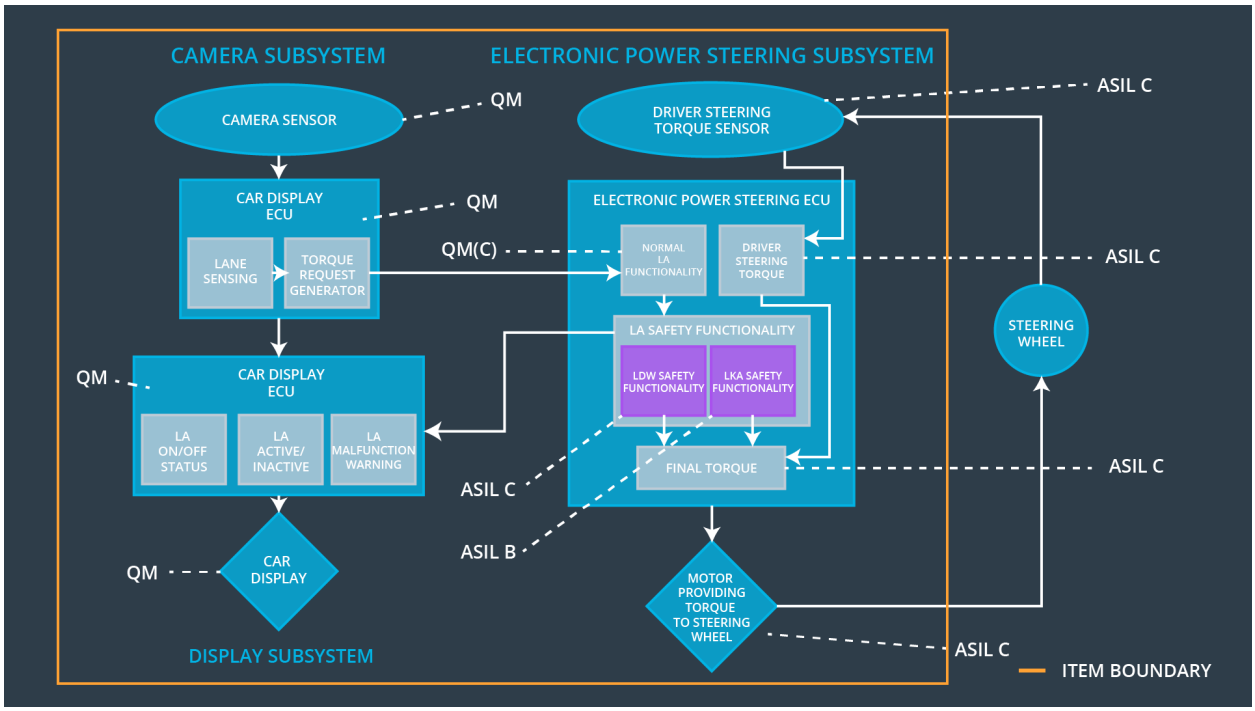
In this document new requirements are defined and assigned to the system architecture. These new requirements are more concrete and gets into details of the item's technology as specified by ISO 26262.

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	Validate that the Max_Torque_Amplitude chosen is low enough that the driver does not loose control over the car.	C	50 ms	Vibration Torque <Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate that the Max_Torque_Frequency chosen is low enough that the driver does not loose control over the car.	C	50 ms	Vibration Frequency < Max_Torque_Frequency
Functional Safety Requirement 02-01	Electronic power steering ECU will ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	LKA_Torque = 0 after time > Max_duration

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Software module detecting the lane line positions from the Camera Sensor images.
Camera Sensor ECU - Torque request generator	Software module calculating the necessary torque to be requested to the Electronic Power Steering ECU.
Car Display	Display warning for the driver.
Car Display ECU - Lane Assistance On/Off Status	Indicate the status of the Lane Assistance 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 activate 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

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 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	LDW Torque Amplitude = 0
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.	C	50 ms	LDW Safety	LDW Torque Amplitude = 0
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	C	50 ms	LDW Safety	LDW Torque Amplitude = 0

	‘LDW_Torque_Request’ 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	LDW Safety	LDW Torque Amplitude = 0
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	LDW Torque Amplitude = 0

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 01-02-01	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request‘ sent to the ‘Final electronically power steering Torque‘ component is below 'Max_Torque_Frequency’	C	50 ms	LDW Safety	LDW Torque Frequency = 0
Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for 'Max_Torque_Frequency’ signal shall be ensured.	C	50 ms	LDW Safety	LDW Torque Frequency = 0

Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'Max_Torque_Frequency‘ shall be set to zero.	C	50 ms	LDW Safety	LDW Torque Frequency = 0
Technical Safety Requirement 01-02-04	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	LDW Torque Frequency = 0
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition Cycle	Data Transmission Integrity Check	LDW Torque Frequency = 0

Lane Keeping Assistance (LKA) Requirements:

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

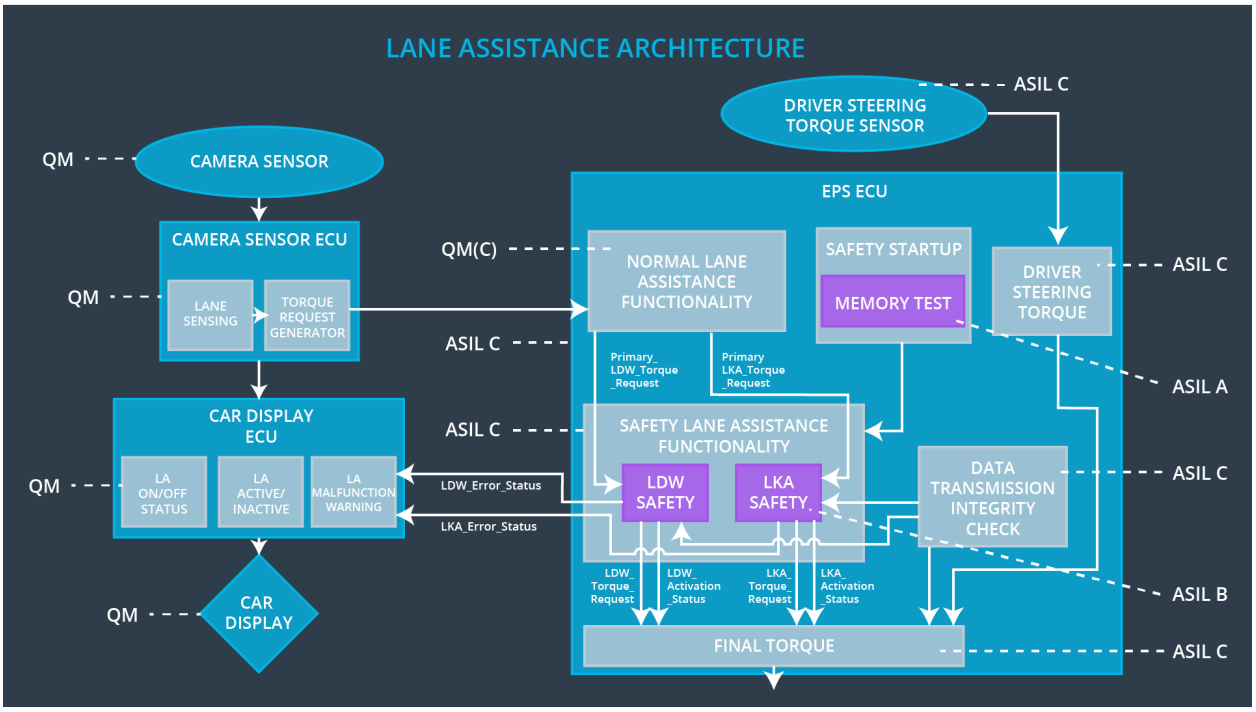
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 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	B	500 ms	LKA Safety	LKA Torque = 0

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.	B	500 ms	LKA Safety	LKA Torque = 0
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.	B	500 ms	LKA Safety	LKA Torque = 0
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	B	500 ms	LKA Safety	LKA Torque = 0
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any memory problems	A	Ignition cycle	Data Transmission Integrity Check	LKA Torque = 0

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 LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request‘ sent to the ‘Final electronically power steering Torque‘ component is below 'Max_Torque_Frequency’	**X**		

Technical Safety Requirement 01-02-02	The validity and integrity of the data transmission for 'Max_Torque_Frequency' signal shall be ensured.	**X**		
Technical Safety Requirement 01-02-03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'Max_Torque_Frequency' shall be set to zero.	**X**		
Technical Safety Requirement 01-02-04	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.	**X**		
Technical Safety Requirement 01-02-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	**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 02-01-04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	**X**		
Technical Safety	Memory test shall be conducted at start up of the EPS ECU to	**X**		

Requirement 02-01-05	check for any memory problems			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off System	Malfunction_01, Malfunction_02,	Yes	Warning indicator on Display unit
WDC-02	Turn off System	Malfunction_03,	Yes	Warning indicator on Display unit