Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
Feb 28, 2018	1.0	Junxun Luo	First Submit

Table of Contents

Purpose of the Technical Safety Concept

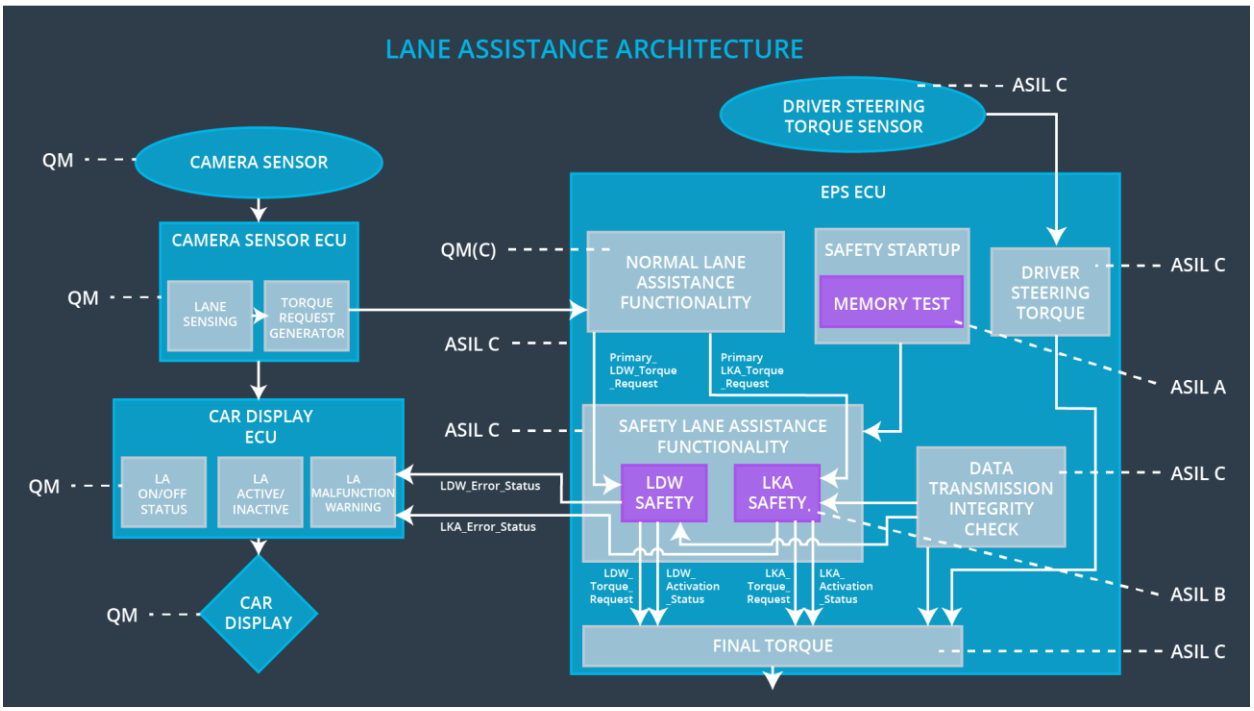
In this document, technical safety requirements are defined and assigned to the system architecture. These requirements are more concrete and gets into details of the item's technology as specified by ISO 26262.

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	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State)	Switch Off Lane Assistance System
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State)	Switch Off Lane Assistance System
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Switch Off Lane Assistance System

Refined System Architecture from Functional Safety Concept



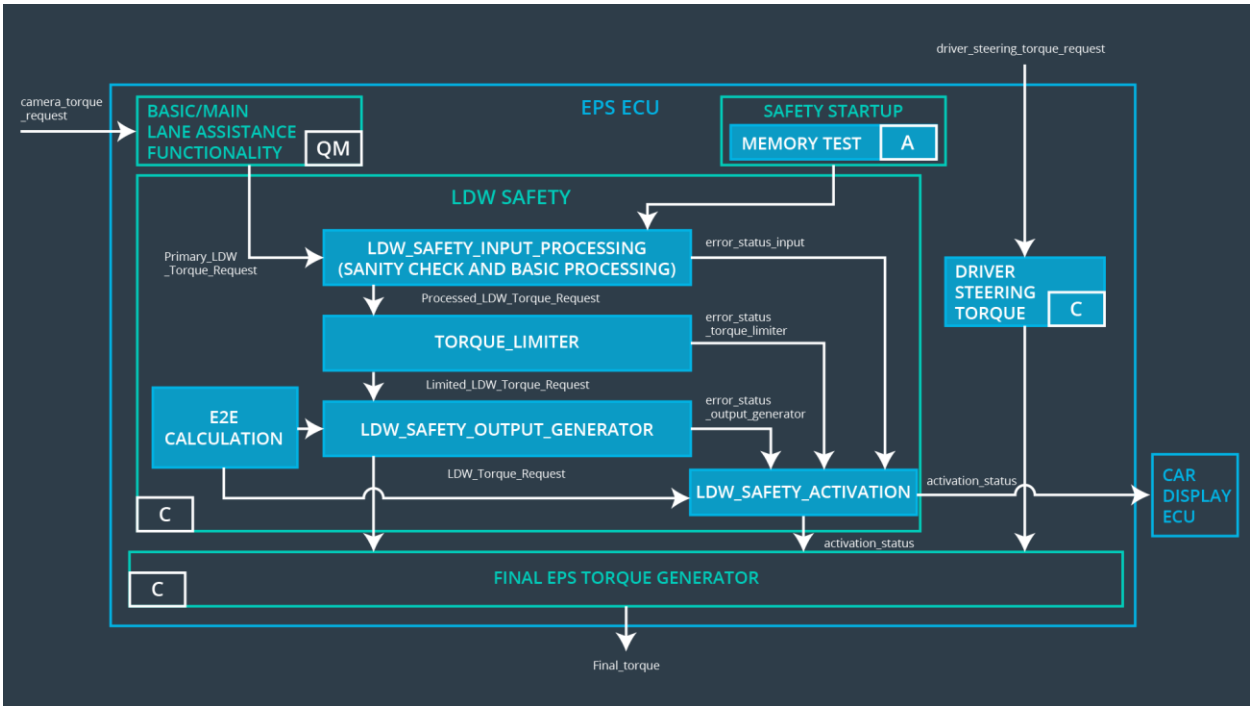
Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Capture 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	Architecture Allocation	Safe State

		L	Interval		
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	Deactivate functionalty (reset Amplitude to 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	Deactivate functionalty (reset Amplitude to 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 'LDW_Torque_Request' to zero.	C	50 ms	LDW Safety	Deactivate functionalty (reset Amplitude to 0)
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	Deactivate functionalty (reset Amplitude to 0)
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	SAFETY STARTUP	Deactivate functionalty (reset Amplitude to 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 Lane Departure Warning safety component shall ensure that the amplitude of the 'LDW_Frequency_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency'.	C	50 ms	LDW Safety	Deactivate functionalty (reset Frequency to 0)
Technical Safety Requirement 01-02-02	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	Deactivate functionalty (reset Frequency to 0)
Technical Safety Requirement 01-02-03	When a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Frequency_Request' to zero.	C	50 ms	LDW Safety	Deactivate functionalty (reset Frequency to 0)
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for 'LDW_Frequency_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Deactivate functionalty (reset Frequency to 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	SAFETY STARTUP	Deactiv ate function alty (reset Frequen cy to 0)

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation	Verify the Lane Departure Warning functionality is turned off.
Technical Safety Requirement 01-01-02	Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION.	Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal.
Technical Safety Requirement 01-01-03	Validate the 'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero.	Verify the Final EPS Torque generator receives a LDW_Torque_Request of zero.
Technical Safety Requirement 01-01-04	Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.
Technical Safety Requirement 01-01-05	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails.
Technical Safety Requirement 01-02-01	Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria.	Verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds Max_Torque_Request.

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:

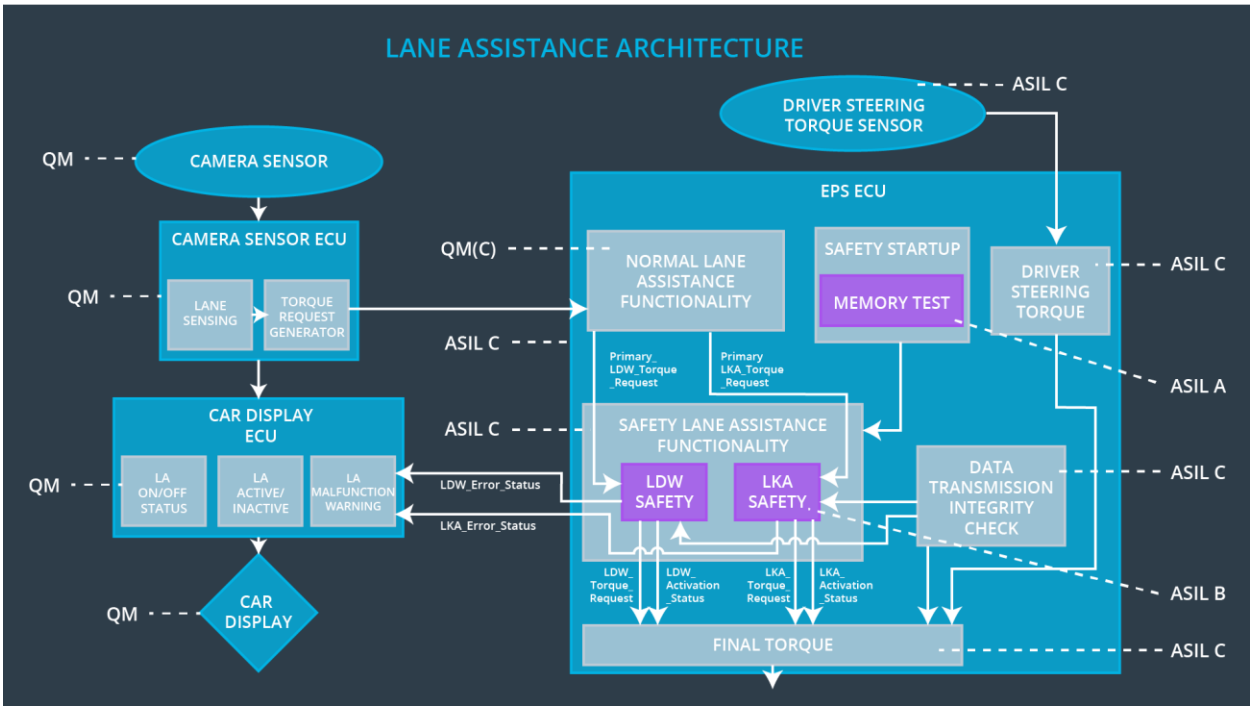
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the Duration of the 'LKA_Duration_Request' sent to the 'Final electronic power steering Torque' component is below Max_Duration	C	50ms	Lane Assistance Safety Functionality	Deactivate functionalty (reset Duration to 0)
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light	C	50ms	LKA Safety Functionality	Deactivate functionality (reset Duration to 0)
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the 'LKA_Duration_Request' shall be set to zero	C	50ms	LKA Safety Functionality	Deactivate functionality (reset Duration to 0)
Technical Safety	The validity and integrity of the data transmission for	C	50ms	Data Transmission	Deactivate functionality

Requirement 04	'LKA_Duration_Request' signal shall be ensured			Integrity Check	(reset Duration to 0)
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	ignition cycle	SAFETY STARTUP	Deactivate functionality (reset Duration to 0)

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	Validate the Max_Torque_Amplitude is the chosen from the Lane Departure Warning Validation	Verify the Lane Departure Warning functionality is turned off.
Technical Safety Requirement 01-01-02	Validate the 'TORQUE_LIMITER' sends the error_status_torque_limiter signal to the LDW_SAFETY_ACTIVATION.	Verify the Car Display ECU displays the Lane Departure Warning malfunction warning signal.
Technical Safety Requirement 01-01-03	Validate the 'TORQUE_LIMITER' sends 'LDW_Torque_Request' with zero.	Verify the Final EPS Torque generator receives a LDW_Torque_Request of zero.
Technical Safety Requirement 01-01-04	Validate the 'TORQUE_LIMITER' calculate and sends the correct cyclic redundancy check (CRC) and Alive counter for data transmission validity and integrity.	Verify the functionality is turn off if there is a CRC or Alive counter discrepancy.
Technical Safety Requirement 01-01-05	Validate the Safety Startup Memory test to check memory faults catch memory faults.	Verify the Lane Departure Warning is turned off when the Safety Startup Memory fails.
Technical Safety Requirement 01-02-01	Validate the Max_Torque_Frequency set is the chosen from the Lane Departure Warning Acceptance Criteria.	Verify the functionality is turned off if the 'LDW_Torque_Request' frequency exceeds Max_Torque_Request.

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	When the Lane Departure Warning is deactivated, the	**X**		

Requirement 01-01-02	'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.			
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 Lane Departure Warning safety component shall ensure the frequency of the 'LDW_Torque_Reques' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'	**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	**X**		

	‘LKA_Torque_Request’ shall be zero.			
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 Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to 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 Lane Departure Warning functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display