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
11/13/2017	1	JP	First Version
11/27/2017	1.1	JP	Minor changes
12/14/2017	2	JP	Second Version

Table of Contents

Purpose of the Technical Safety Concept

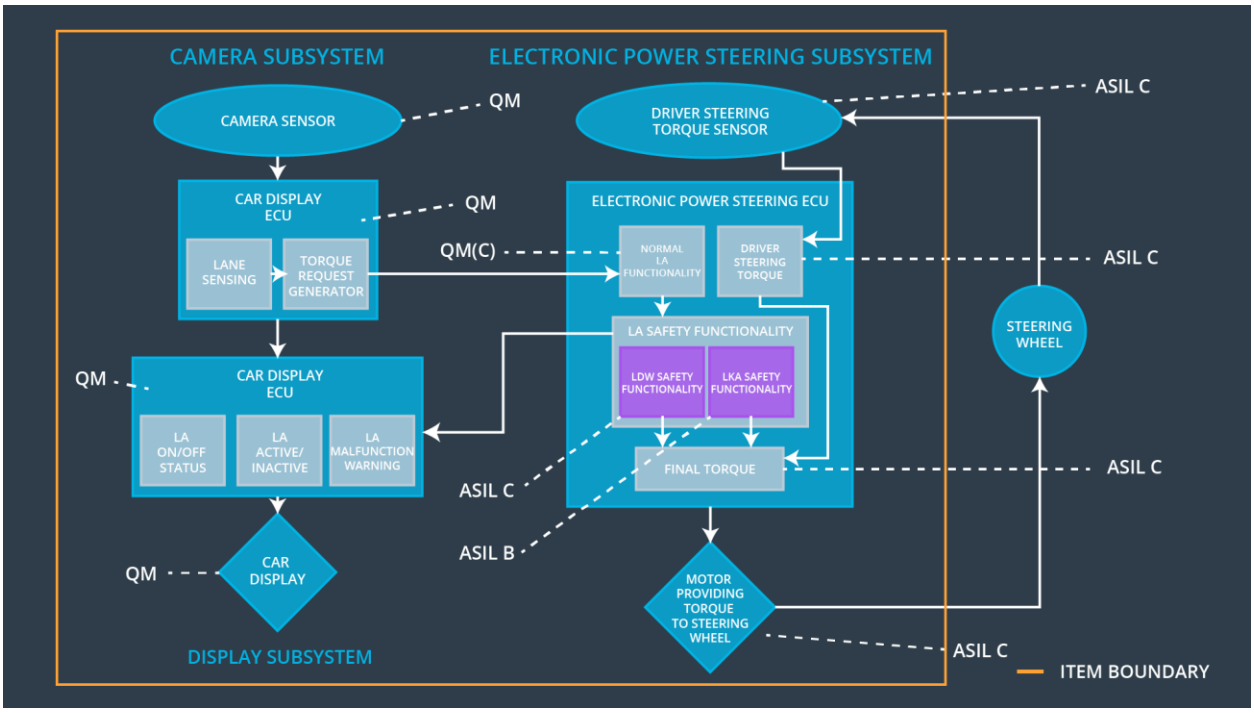
The purpose of the technical safety concept is generally similar to the functional safety concept. It will identify new requirements and allocate them to the system architecture. The difference it, that the technical safety concept is looking at a system at a more detailed level and is concrete than the function safety concept. Is looks at safety requirements of sensors, control units and actuators.

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 LDW shall ensure that the lane departure oscillating torque amplitude is below MAX_Torque_Amplitude	C	50 ms	Set vibration torque amplitude to 0
Functional Safety Requirement 01-02	The LDW shall ensure that the lane departure oscillating torque frequency is below MAX_Torque_Frequency	C	50 ms	Set vibration torque frequency 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	Set lane keeping assistance torque to 0
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to Car Display	B	500 ms	Set lane keeping assistance torque to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Is taking and sending an image stream to the camera sensor ECU
Camera Sensor ECU - Lane Sensing	Software Module in the Camera Sensor ECU responsible for detecting lane lines and determining when the vehicles leaves the lane by mistake.
Camera Sensor ECU - Torque request generator	Software Module in the Camera Sensor ECU responsible for calculating and sending the additional torque for the LDW and LKA functions
Car Display	Is a visual display responsible for displaying warnings of lane departures and LKA activation and deactivation.

Car Display ECU - Lane Assistance On/Off Status	Visual display responsible for displaying LKA and LDW ON/OFF status.
Car Display ECU - Lane Assistant Active/Inactive	Visual display responsible for displaying warning of lane departures, LKA and LDW activations and deactivations.
Car Display ECU - Lane Assistance malfunction warning	Visual display responsible for displaying warning of LKA and LDW malfunctions.
Driver Steering Torque Sensor	Is responsible for measuring the torque provided by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software Module in the electronic power steering ECU responsible for receiving the Camera Sensor ECU torque request.
EPS ECU - Normal Lane Assistance Functionality	Software Module in the Electronic Power Steering ECU responsible for receiving the Driver Steering Torque Sensor input from the steering wheel
EPS ECU - Lane Departure Warning Safety Functionality	Software module in the electronic power steering ECU responsible for keeping the lane departure oscillating torque amplitude and frequency below MAX_Torque_Amplitude and MAX_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module in the electronic power steering ECU responsible for ensuring the application of the lane keeping assistance torque does not ever exceeded Max_Duration and if lane detection is lost, the LKA function is deactivated.
EPS ECU - Final Torque	Software module in the electronic power steering ECU responsible for ensuring the LDW, LKA and the driver’s steering torque requests are combined and sent to the motor.
Motor	Is executing the torque request of the electronic power steering ECU and provides torque 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	Set LDW torque to zero
Technical Safety	As soon as the LDW function	C	50 ms	LDW Safety block	Set LDW torque to zero

Requirement 01-01-02	deactives the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.				
Technical Safety Requirement 01-01-03	As soon as a failure is detected by the LDW function, it shall deactive the LDW feature and the 'LDW_Torque_Request' shall be set to zero.	C	50 ms	LDW safety block	Set LDW torque 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	Set LDW torque to zero
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	Memory Test	Set LDW torque 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 01-02-01	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_Frequency	C	50 ms	LDW Safety block	Set LDW torque to zero
Technical Safety Requirement 01-02-02	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	Set LDW torque to zero
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 LDW_Torque_Request shall be set to zero.	C	50 ms	LDW Safety block	Set LDW torque to zero
Technical Safety Requirement 01-02-04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured.	C	50 ms	Data transmission integrity check	Set LDW torque to zero
Technical Safety Requirement 01-02-05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	Set LDW torque to zero

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement	Validate that the Max_Torque_Amplitude set is the	Verify that the system really does turn off if the lane departure warning LDW_Torque_Request ever exceeded

01-01-01	chosen from LDW validation Acceptance criteria.	Max_Torque_Amplitude
Technical Safety Requirement 01–01-02	Validate that the Torque_Limiter in the LDW Safety software block sends the error_status_torque_limiter signal to the LDW_Safety_Activation	Verify that the Car display ECU displays the LDW malfunction warning light.
Technical Safety Requirement 01-01-03	Validate that the TORQUE_LIMITER in the LDW Safety software block sends a zero LDW_Torque_Request	Verify that the Final EPS TORQUE Generator receives a 0 LDW_Torque_Request
Technical Safety Requirement 01-01-04	Validate that the Torque_Limiter in the LDW Safety software block calculate and sends a correct CRC and Alive counter for data transmission validity and integrity	Verify that the system really does turn off if the lane departure warning LDW_Torque_Request ever has an invalid CRC or Alive counter.
Technical Safety Requirement 01-01-05	Validate that the safety startup memory test to check memory faults will catch memory faults	Verify that de LDW system really does turn off if the Safety Startup Memory test fails
Technical Safety Requirement 01-02-01	Validate that the Max_Torque_Frequency set is the chosen from LDW Validation Acceptance Criteria	Verify that the system really does turn off if the lane departure warning LDW_Torque_Request ever exceeded Max_Torque_Frequency

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	X		

	only Max_Duration			

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 shall ensure that the duration of the keeping assistance torque applied is less than Max_Duration	B	500 ms	LKA safety block	Set LKA torque to zero
Technical Safety Requirement 02-01-02	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	B	500 ms	LKA safety block	Set LKA torque to zero
Technical Safety Requirement 02-01-03	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 block	Set LKA torque to zero
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	Data transmission integrity check	Set LKA torque to zero
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory	A	Ignition cycle	Safety startup - Memory test	Set LKA torque to 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	The electronic power steering	X		

Safety Requirement 02-02	ECU shall ensure that the lane keeping assistance torque is set to zero when the camera sensor ECU stops detecting road markings and shall send its off status to the Car display			

Technical Safety Requirements related to Functional Safety Requirement 02-02 are:

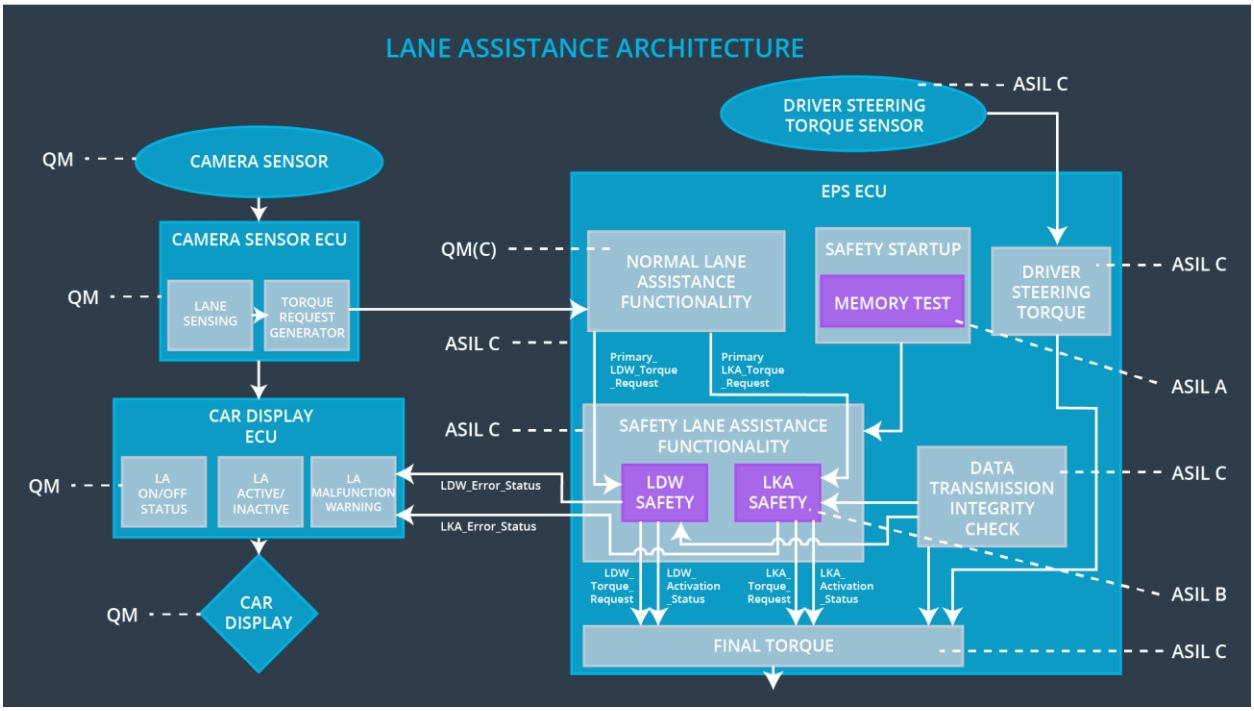
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 02-02-01	The LKA safety component shall ensure that the loss of camera sensor torque request transmission will deactivate the LKA feature and the LKA_Torque_Request shall be set to zero	C	500 ms	LKA safety block	Set LKA torque to zero

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-01-01	Validate that the Max_Duration set is the chosen from LKA Validation Acceptance Criteria	Verify that the system really does turn off if the LKA_Torque_Request ever exceeded Max_Duration
Technical Safety Requirement 02–01-02	Validate that the Torque_Limiter in the LDW Safety software block sends the error_status_torque_limiter signal to the LKA_Safety_Activation	Verify that the car display ECU displays the LKA malfunction warning light.
Technical Safety Requirement 02-01-03	Validate that the TORQUE_LIMITER in the LKA Safety software block sends a zero LKA_Torque_Request.	Verify that the Final EPS Torque generator receives a 0 LKA_Torque_Request.
Technical Safety Requirement	Validate that the TORQUE_LIMITER in the LKA Safety software block calculate and send a correct CRC and Alive	Verify that the system really does turn off if the lane keeping assistance LKA_Torque_Request ever has an

02-01-04	counter for data transmission validity and integrity	invalid CRC or Alive counter.
Technical Safety Requirement 02-01-05	Validate that the safety startup memory test to check memory faults will catch memory faults	Verify that de LKA system really does turn off if the Safety Startup Memory test fails
Technical Safety Requirement 02-02-01	Validate that the camera ECU sense zero LKA_Torque_Request when it fails to detect lane lines and stop Alive counter for data transmission validity and integrity	Verify that the system really does turn off if the lane keeping assistance LKA_Torque_Request ever has an invalid CRC or Alive counter failure from the camera ECU

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

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	Turn off LDW functionality	Malfunction_01, Malfunction_02, Malfunction_04	Yes	LED on car display
WDC-02	Turn off LKA functionality	Malfunction_03, Malfunction_05	Yes	LED on car display