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
06-11-2017	1.0	S.Chonavel	Initial version

Table of Contents

Purpose of the Technical Safety Concept

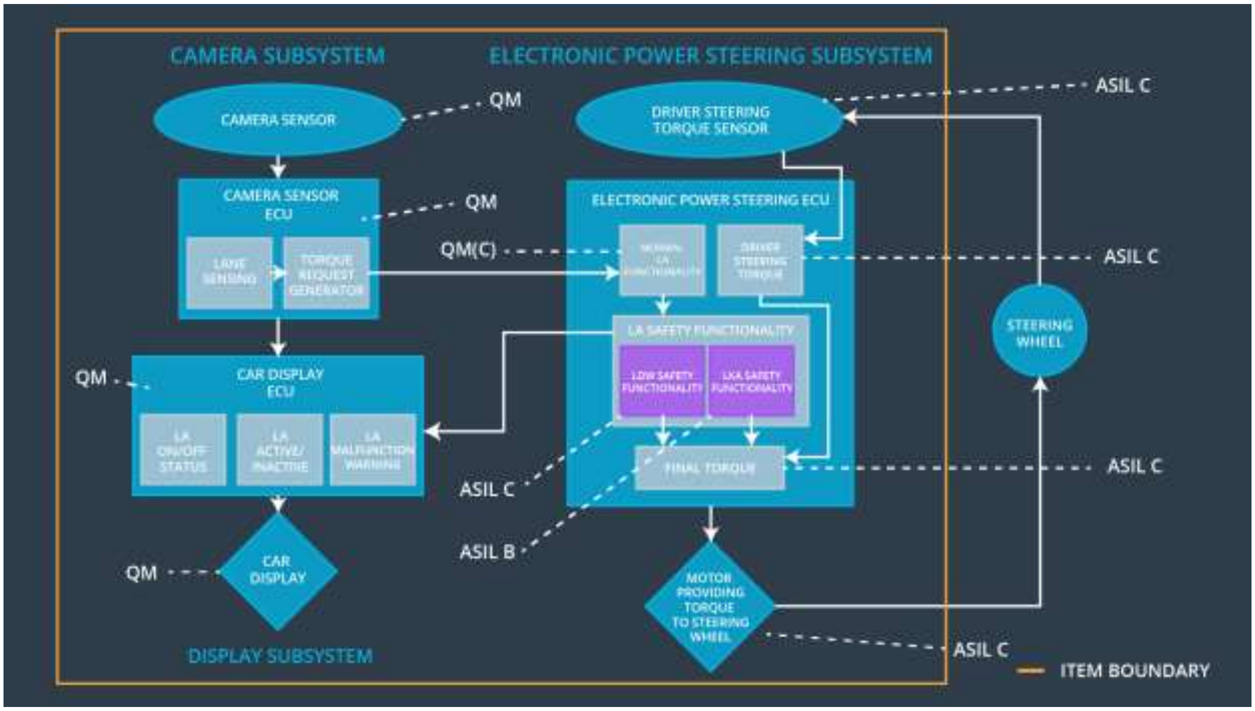
This document describes at system level how the subsystem interact and allocate system safety level requirement at subsystem level.

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 oscillating steering wheel torque shall be below a specified limits.	C	50ms	Set vibration torque amplitude to zero. Warn user of LDW malfunction
Functional Safety Requirement 01-02	The oscillating steering wheel torque shall be above a specified limits.	B	50ms	Set vibration torque amplitude to zero Warn user of LDW malfunction
Functional Safety Requirement 02-01	The lane keeping Assistance shall be limited in time.	B	500ms	System is turned off. Warn user that LKA function is off
Functional Safety Requirement 02-02	The lane keeping assistance shall apply torque within a limited time.	B	50ms	System is turned off. Warn user of LKA malfunction

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Capture and transmit an image of the vehicle frontal area.
Camera Sensor ECU - Lane Sensing	• Analyses the camera sensor output and determine the position of the vehicle with respect to the lane. • Inform the Torque request generator in case of a lane departure situation. • Inform the display System in case of lane departure.
Camera Sensor ECU - Torque request generator	• Compute the torque request in case of lane departure • Generate torque request to the Power Steering ECU in case of a lane departure situation.
Car Display	Display the lane departure signal to the driver or the LDW and LKA status (on or off).

Car Display ECU - Lane Assistance On/Off Status	Display to the driver either the message “Lane assistance on” or the message “Lane assistance off”
Car Display ECU - Lane Assistant Active/Inactive	Display to the driver either the message “Lane assistance Active” or the message “Lane assistance Not Active”
Car Display ECU - Lane Assistance malfunction warning	Display to the driver the message “Lane assistance Malfunction” warning message”
Driver Steering Torque Sensor	Reads the steering torque exerted by the driver on the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	• Receives information from the “Driver Steering Torque Sensor” • Receives torque request from the “Camera Sensor ECU” • Compute the requested “motor torque” • Generate torque request command to the “steering wheel motor” • Generate a waning request to the car display ECU when appropriate.
EPS ECU - Normal Lane Assistance Functionality	Receives Torque request from the “Camera sensor ECU”
EPS ECU - Lane Departure Warning Safety Functionality	Check the validity of the steering oscillation torque and frequency request validity and either push them through or generate a “Malfunction warning” signal request to the “Car display ECU”
EPS ECU - Lane Keeping Assistant Safety Functionality	Check the validity of the “torque request” to help steer the vehicle back in lane.
EPS ECU - Final Torque	• Compute the torque resulting from : o the LDW request o the LKA requests o the driver steering torque • Transmit the result to the “steering wheel motor”
Motor	Generates the steering torque as per “EPS-ECU” request

Technical Safety Concept

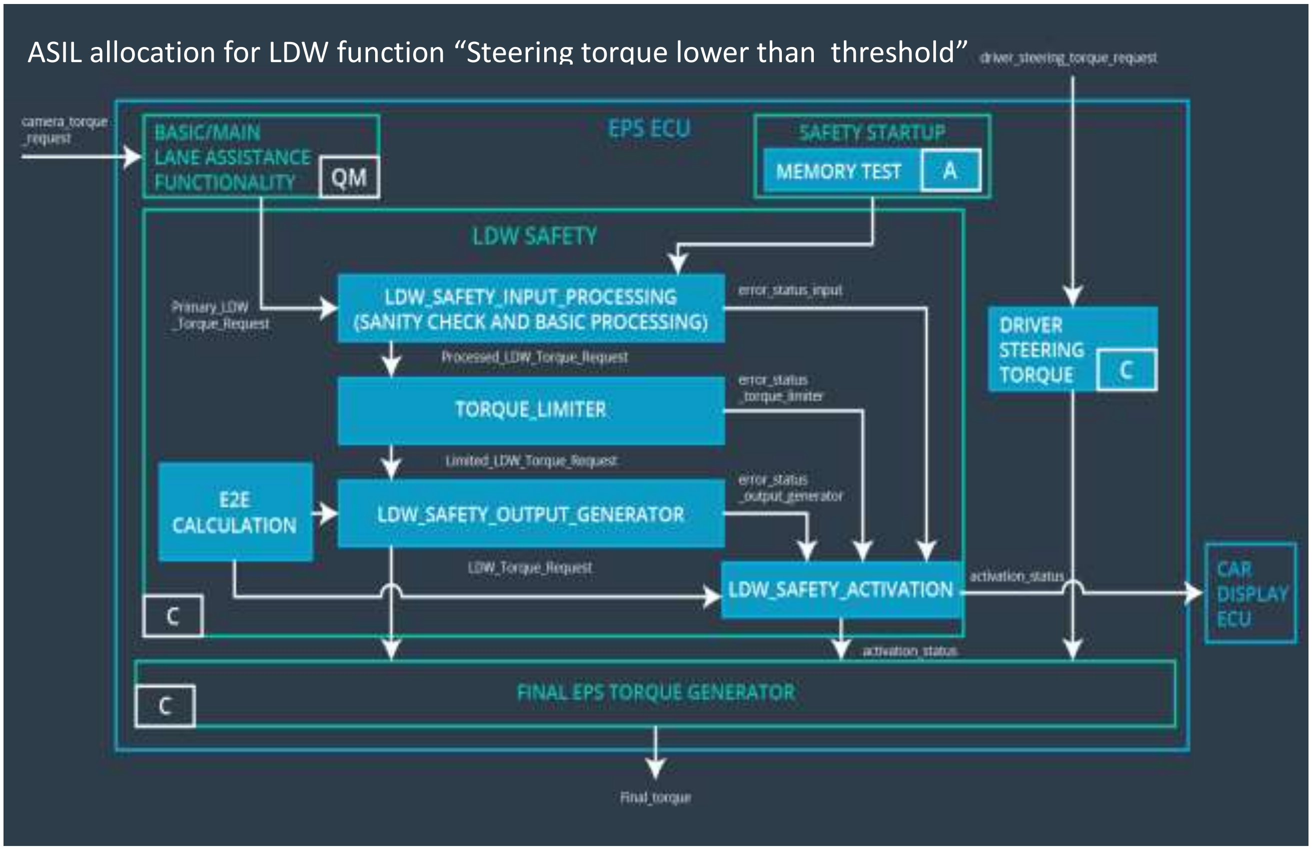
Technical Safety Requirements

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:

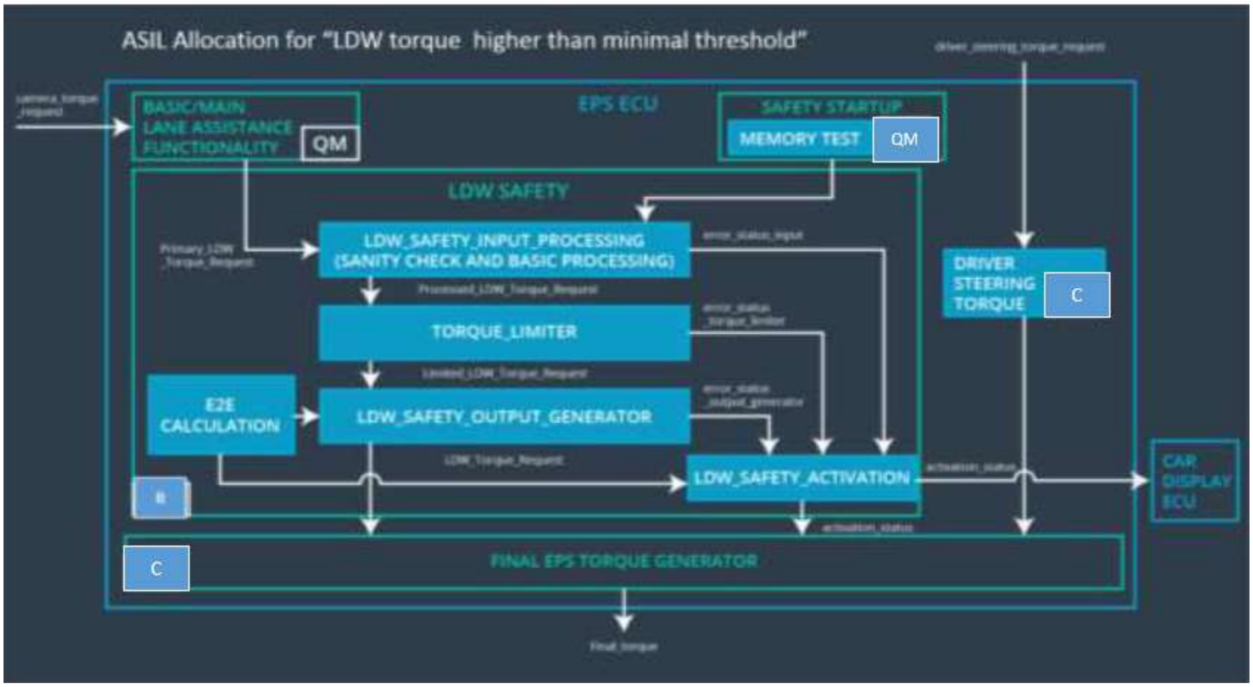

ASIL allocation for LDW function “Steering torque lower than threshold”

driver_steering_torque_request
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
A
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
DRIVER STEERING TORQUE
C
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
C
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

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	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction
Technical Safety Requirement 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 ligh	C	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction
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	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction
Technical Safety Requirement 04	The validity and integrity of the data transmission for LDW_Torque_Request signal shall be ensured	C	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup block	Set LDW to zero. Warn user of LDW malfunction

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 oscillating steering wheel torque shall be above a specified limits.	X		


ASIL Allocation for "LDW torque higher than minimal threshold"
driver_steering_torque_request
camera_torque_request
EPS ECU
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
SAFETY STARTUP
MEMORY TEST
QM
LDW SAFETY
Primary_LDW_Torque_Request
LDW_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LDW_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LDW_Torque_Request
E2E CALCULATION
LDW_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LDW_Torque_Request
LDW_SAFETY_ACTIVATION
activation_status
B
DRIVER STEERING TORQUE
C
CAR DISPLAY ECU
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is above 'Min_Torque_Amplitude.	B	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user

					of LDW malfunction
Technical Safety Requirement 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 on	B	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction
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.	B	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	LDW Safety block	Set vibration torque amplitude to zero. Warn user of LDW malfunction

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	Check that the torque limiter reference “correspond to the”Max_torque_Amplitude” specified.	Check the state ofthe “error_status_torque_limiter” value in case of “primary LDW torque Request” too high
Technical Safety Requirement 01-01-02	Check that any error form either : - “error_status_input” - “error_status_torque_limiter” - “error status_output_generator_ - ECE calculation fault Change the states of the	Check that any of those errors will: - Generate a request is sent to the car display ECU - Set the “final torque” request to zero

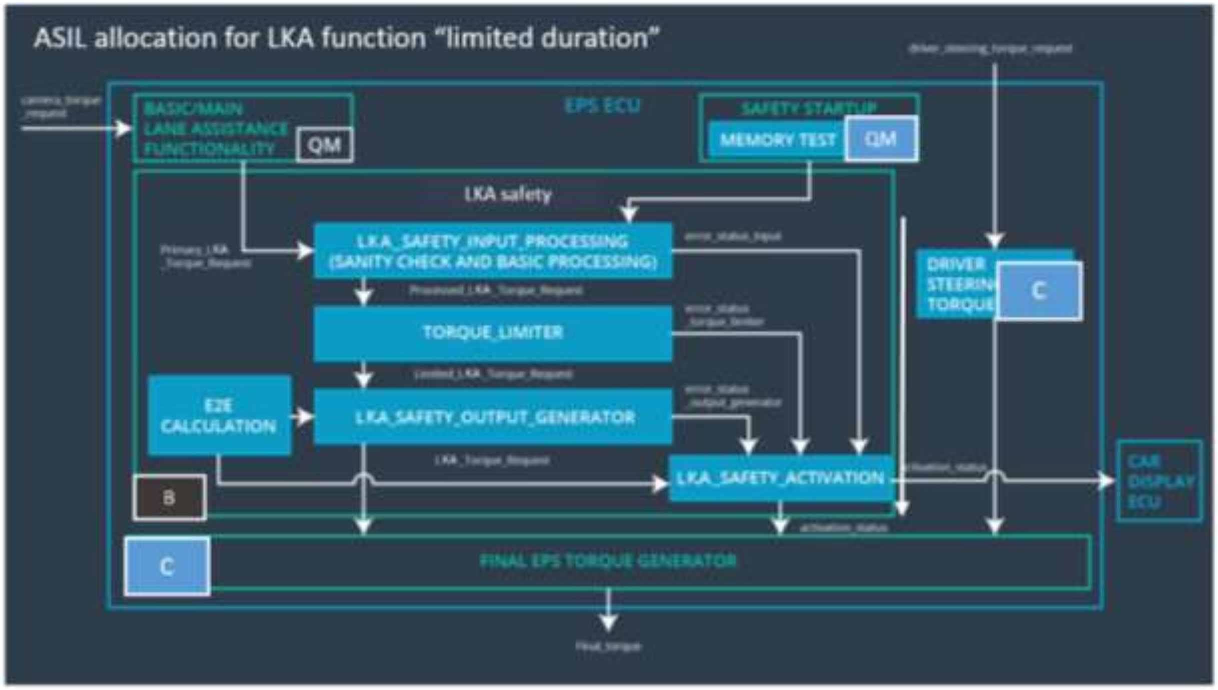
	“activation_status”	
Technical Safety Requirement 01-01-03	Check that an “ECE Calculation” error will lead to: - a ”LDW Torque request of zero” - an “error status output generator” shift - an “activation _status” shift	Check that and E2E error will: - Generate a request is sent to the car display ECU - Set the “final torque” request to zero
Technical Safety Requirement 01-01-04	Check that : - The max torque limit from the memory is the same as the one in the “Torque limiter”	Check that a failed memory test will: - Generate a request is sent to the car display ECU - Set the “final torque” request to zero
Technical Safety Requirement 01-02-01	Check that the torque limiter reference “correspond to the”Min_torque_Amplitude” specified.	Check the state of the “error_status_torque_limiter” value in case of “primary LDW torque Request” too low

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:


ASIL allocation for LKA function "limited duration"
camera_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
QM
driver_steering_torque_request
LKA safety
Primary_LKA_Torque_Request
LKA_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Processed_LKA_Torque_Request
TORQUE_LIMITER
error_status_torque_limiter
Limited_LKA_Torque_Request
E2E CALCULATION
LKA_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LKA_Torque_Request
DRIVER STEERING TORQUE
C
B
LKA_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

ID	Technical Safety Requirement	A S I L	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that LDA is active for less than "Max_duration"	B	500ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction
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 on	B	500ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction
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	500ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction

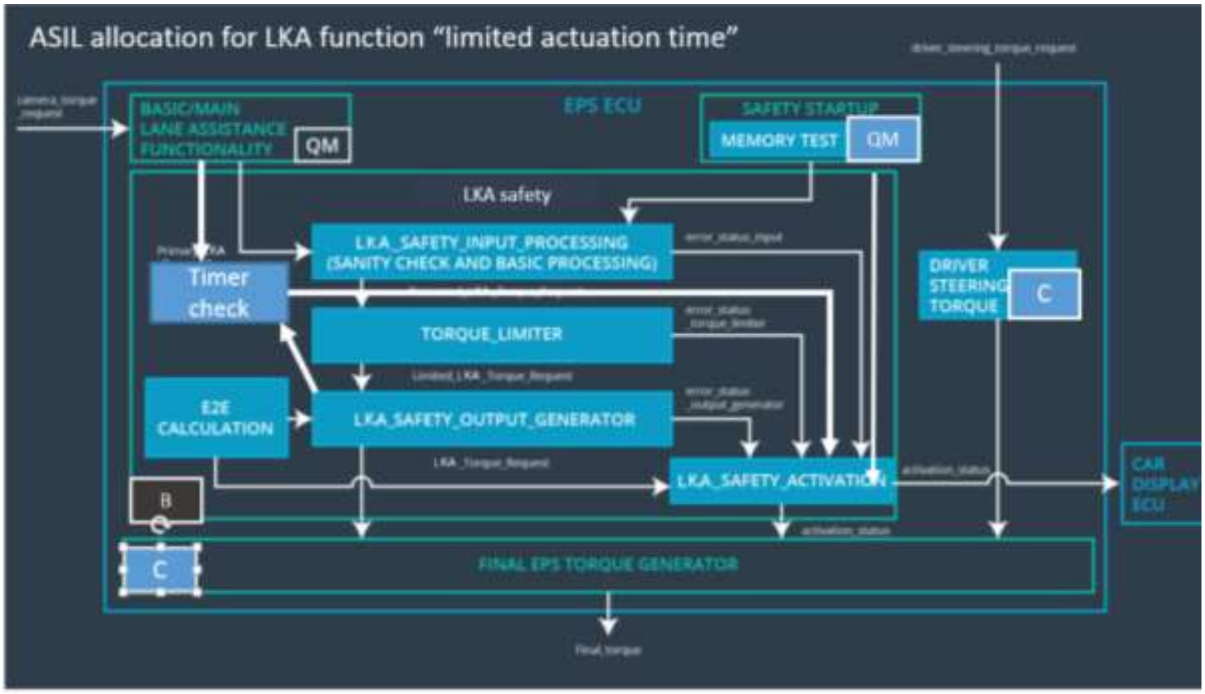
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	QM	Ignition cycle	Safety Startup block	Set LKA to zero. Warn user of LKA malfunction

Functional Safety Requirement 02-2 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 02-02	The lane keeping assistance shall apply torque within a limited time.	X		

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

Note: the architecture schematics has been modified to include a “timer block” used to check both the Max_active time as well as the execution time of the LKA function.



ASIL allocation for LKA function "limited actuation time"

camera_torque_request
driver_steering_torque_request
BASIC/MAIN LANE ASSISTANCE FUNCTIONALITY
QM
EPS ECU
SAFETY STARTUP
MEMORY TEST
QM
LKA safety
LKA_SAFETY_INPUT_PROCESSING (SANITY CHECK AND BASIC PROCESSING)
error_status_input
Timer check
DRIVER STEERING TORQUE
C
TORQUE_LIMITER
error_status_torque_limiter
Limited_LKA_Torque_Request
E2E CALCULATION
LKA_SAFETY_OUTPUT_GENERATOR
error_status_output_generator
LKA_Torque_Request
LKA_SAFETY_ACTIVATION
activation_status
CAR DISPLAY ECU
B
activation_status
C
FINAL EPS TORQUE GENERATOR
Final_torque

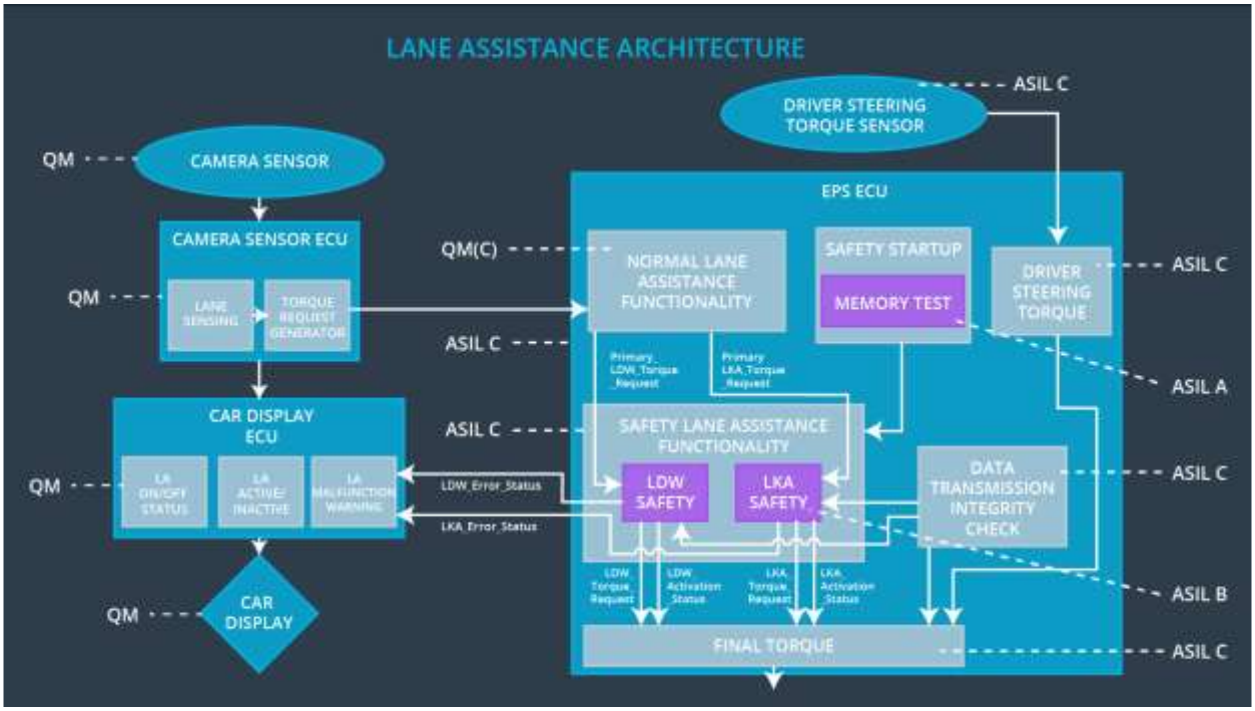
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the actuation time is lower than "Max_actuation time"	B	50ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction
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 on	B	50ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction
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	50ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	50ms	LKA Safety block	Set torque request to zero. Warn user of LKA malfunction
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	QM	Ignition cycle	Safety Startup block	Set LKA to zero. Warn user of LKA malfunction

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	Check that the “LKA max active time reference “correspond to the”Max_time” specified.	Check that if the “Max time” is passed - A warning message is displayed - The final_torque value is zero
Technical Safety Requirement 01-01-02	Check that any error form either : - “error_status_input” - “error_status_torque_limiter” - “error status_output_generator_ - ECE calculation fault Change the states of the “activation_status”	Check that any of those errors then: - A warning message is displayed - The final_torque value is zero
Technical Safety Requirement 01-01-03	Check that an “ECE Calculation” error will lead to: - a ”LDW Torque request of zero” - an “error status output generator” shift - an “activation _status” shift	Check that if this error happened then: - A warning message is displayed - The final_torque value is zero
Technical Safety Requirement 01-01-04	Check that : - The max time limit from the memory is the same as the one in the “Timer block”	Check that a failed memory test will lead to : - A warning message is displayed - The final_torque value is zero
Technical Safety Requirement 01-02-01	Check that the max_actuation_time stored in the “timer block“ correspond to the ”Min_actuation time” specified.	Check thant is this actuation time is exceeded then : - A warning message is displayed - The final_torque value is zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	EPS ECU – Safety Lane Assistance Functionality	EPS ECU – Data Trans. Integrity Check	EPS ECU – Safety startup
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 'Min_Torque_Amplitude.	X		
Technical Safety Requirement 01-01-02	As soon as the LDW function deactivates the LDW feature, the 'LDW Safety' software block	X		

	shall send a signal to the car display ECU to turn on a warning light on			
Technical Safety Requirement 01-01-03	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.	**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 startup of the EPS ECU to check for any faults in memory.			**X**
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 above 'Min_Torque_Amplitude.	**X**		
Technical Safety Requirement 02-01-01	The LKA safety component shall ensure that LDA is active for less than “Max_duration”	**X**		
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 on	**X**		
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.	**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 Requirement 02-02-01	The LKA safety component shall ensure that the actuation time is lower than “Max_actuation time”	**X**		

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	LDW function is off	Malfunction 01-01,01-02	Yes LDW is off	Yes A LDW warning message is displayed on the car display
WDC-02	LKA function is off	Malfunction 02-01,02-02	Yes LKA is off	Yes A LKA warning message is displayed on the car display