Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
2019.06.28	1.0	Yuan.J	Initial Draft

Table of Contents

Purpose of the Technical Safety Concept

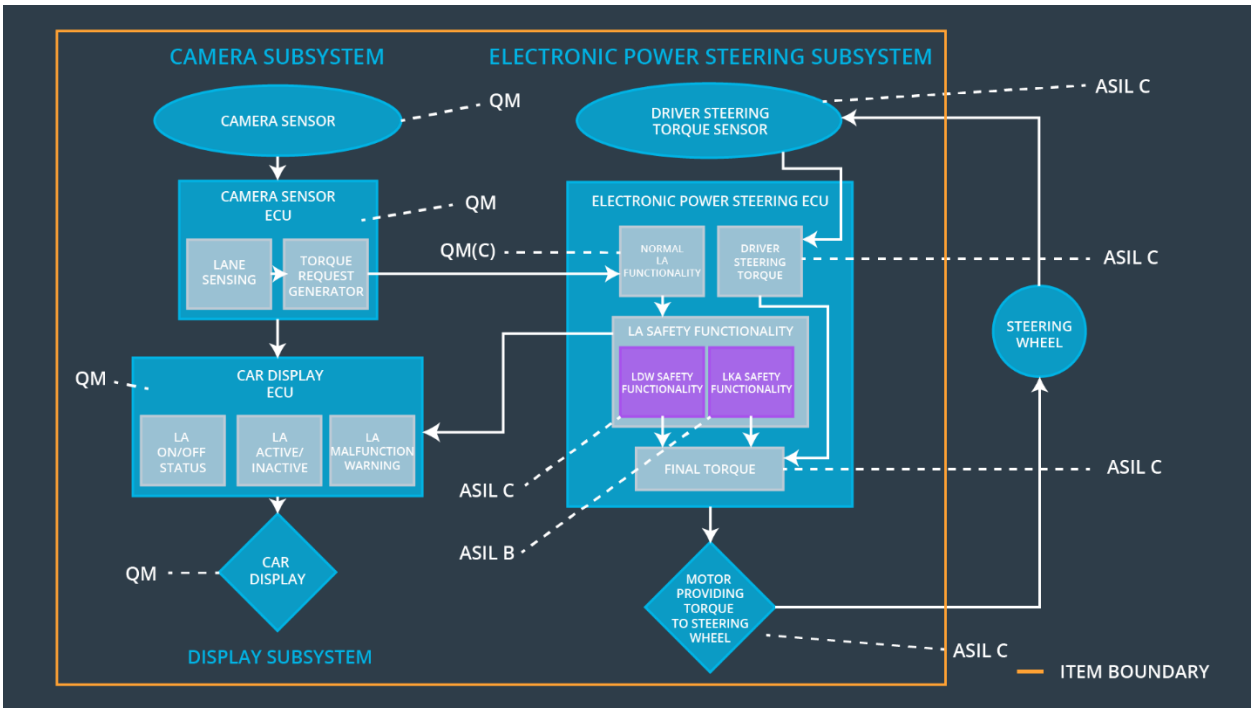
The purpose of the technical safety concept is to turn functional safety requirements into concrete and detail requirements. It allocates the technical safety requirements to the system architecture and describes in detail what the system shall do when a malfunction violates a safety goal.

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 Electronic Power Steering ECU shall ensure that the oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude	C	50ms	LDW will set the oscillating torque amplitude to zero
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the oscillating torque frequence requested by the LDW function is below Max_Frequence_Amplitude	C	50ms	LDW will set the oscillating torque amplitude to zero
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	500ms	Set lane keeping Assistance torque to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Provide the raw input (images) for the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Process the raw images and detect the lane lines and if the vehicle stays in the lane.
Camera Sensor ECU - Torque request generator	Camera Sensor ECU responsible for calculating and sending the additional torque to the acuator.
Car Display	Visual display responsible to displaying warning of lane departures and LKA and LDW state.
Car Display ECU - Lane Assistance On/Off Status	Responsible to displaying LKA and LDW ON/OFF status
Car Display ECU - Lane Assistant Active/Inactive	Responsible to displaying warning of lane assist activation and deactivations states.
Car Display ECU - Lane Assistance malfunction warning	Responsible to displaying warning of LKA and LDW malfunctions.
Driver Steering Torque Sensor	Sensor responsible for measuring of the steering torque which the driver is applying to the steering

	wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Responsible for receiving the Camera Sensor ECU torque requests and output the Torque request to the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Processes the generated Torque Request by the Camera Sensor ECU and forwards it to the LA Safety Functionality
EPS ECU - Lane Departure Warning Safety Functionality	Responsible for keeping the lane departure oscillating torque amplitude and frequence below MAX_Torque_Amplitude and MAX_Torque_Fequency respectively.
EPS ECU - Lane Keeping Assistant Safety Functionality	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	Final torque output that is to applied to the steering wheel.
Motor	Generates output torque for additional steering torque applied 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	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 the oscillating torque amplitude to zero
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.	C	50 ms	LDW Safety block	Set lane departure warning torque 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 block	Set lane departure warning torque to zero
Technical Safety Requirement 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 lane departure warning torque 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	Ignition cycle	Memory Test Block	Set lane departure warning 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	The lane keeping item shall ensure that the lane departure oscillating torque frequency is	X		

01-02	below Max_Torque_Frequency			

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 fequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Fequency'	C	50 ms	LDW Safety block	Set lane departure warning torque to zero
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.	C	50 ms	LDW Safety block	Set lane departure warning torque 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 block	Set lane departure warning torque to zero
Technical Safety Requirement 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 lane departure warning torque 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	Ignition cycle	Memory Test Block	Set lane departure warning torque to zero

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety	Validate if the MAX_Torque_Amplitude chosen is appropriate by testing with	Verify that the system really does turn off if the lane departure warning ever

Requirement 01-01	different drivers' reaction to different torque amplitudes.	exceeded MAX_Torque_Amplitude
Functional Safety Requirement 01-02	Validate if the Max_Torque_Frequency chosen is appropriate by testing with different drivers' reaction to different torque amplitudes.	Verify that the system really does turn off if the lane departure warning ever exceeded MAX_Torque_Fequency

Lane Keeping Assistance (LKA) Requirements:

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

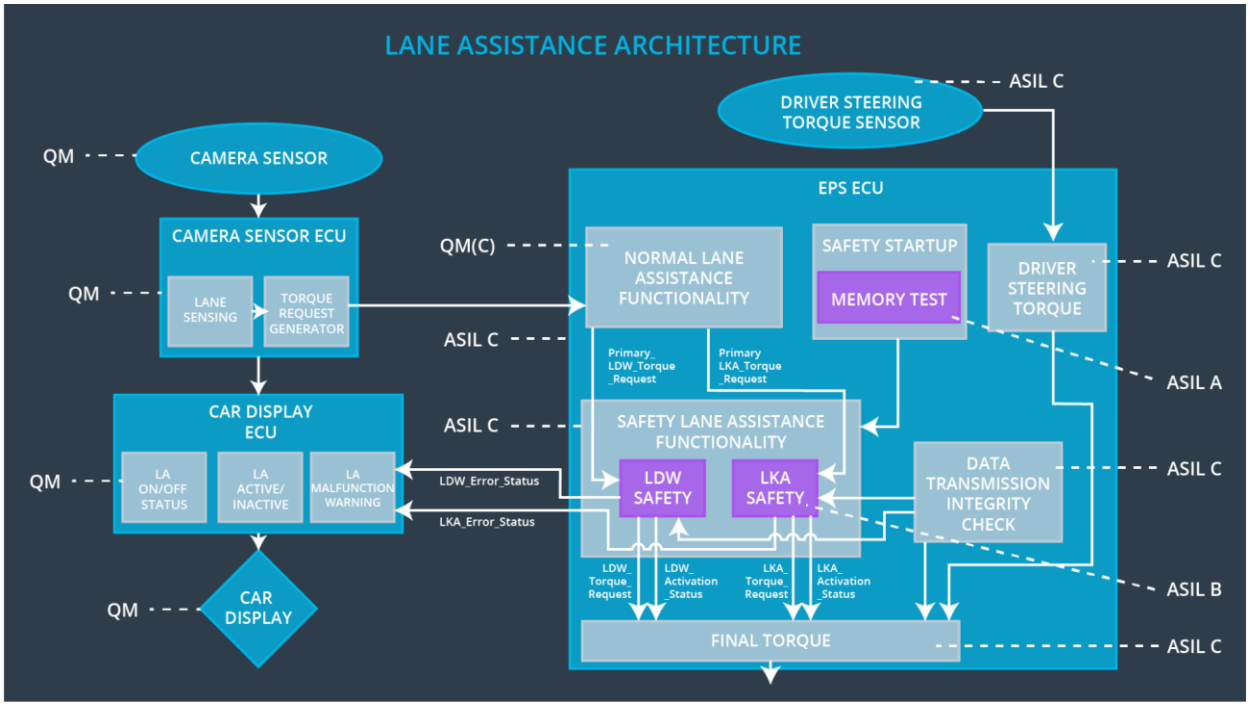
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 lane keeping assistance torque applied is less than Max_Duration.	B	500ms	LKA Safety block	Set lane keeping assistance torque to zero
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.	B	500ms	LKA Safety block	Set lane keeping assistance torque 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	500ms	LKA Safety block	Set lane keeping assistance torque to zero

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity Check	Set lane keeping assistance torque to zero
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	Memory Test Block	Set lane keeping assistance torque to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item 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	Torque amplitude is higher than Max_Torque_Amplitude	Yes, LDW torque shall be set to zero	LDW Inactive and Malfunction Warning will be display at the vehicle dashboard.
WDC-02	Turn off LDW functionality	Torque frequency is higher than Max_Torque_Frequency	Yes, LDW torque shall be set to zero	LDW Inactive and Malfunction Warning will be display at the vehicle dashboard.
WDC-03	Turn off LKA functionality	Duration of torque application is higher than ‘Max_Duration’	Yes, LKA torque shall be set to zero	LKA Inactive and Malfunction Warning will be display at the vehicle dashboard.