Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
05/12/18	1.0	Diogo Leal	First submission

Table of Contents

Purpose of the Technical Safety Concept

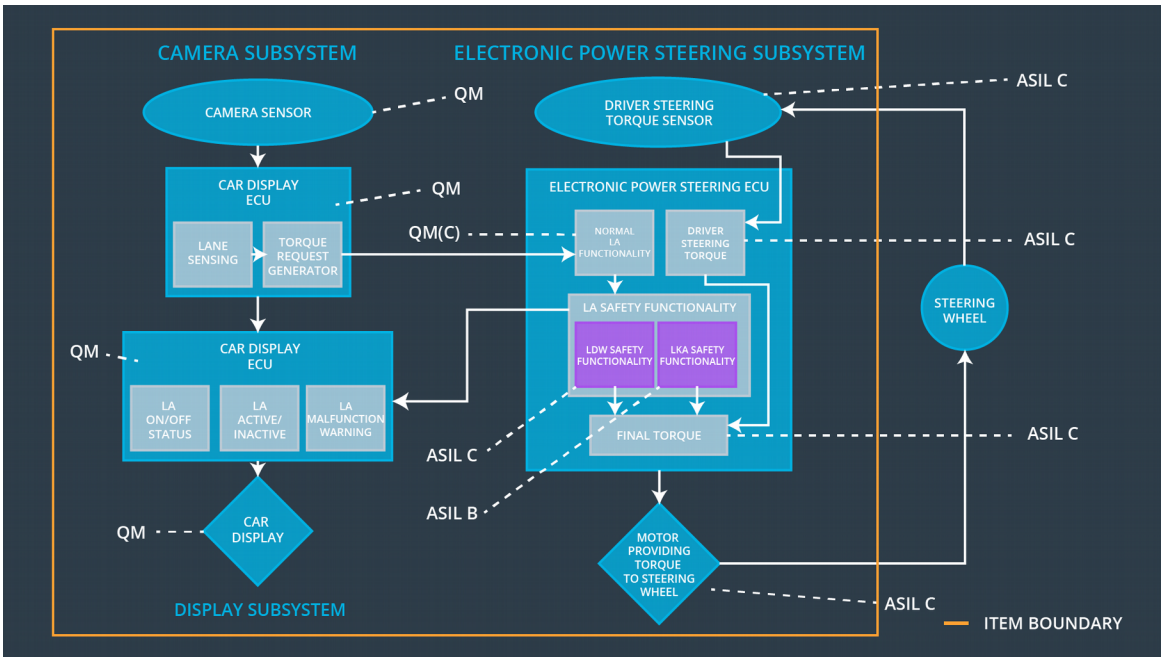
The purpose of the Technical Safety Concept is to develop requirements that cover how sensors, control units and actuators should interact between them to ensure funcitonal safety.

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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Oscillating torque from LDW function is set to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Oscillating torque from LDW function is set 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	Torque request from the LKA function is set to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures images from the road
Camera Sensor ECU - Lane Sensing	Detects lanes on the road and when the driver leaves the lane
Camera Sensor ECU - Torque request generator	Sends torque request to the Electronic Power Steering Subsystem
Car Display	Lights that alerts the driver about the system current state
Car Display ECU - Lane Assistance On/Off Status	Controls the light that tells the driver if the Lane Keeping Item is On or Off
Car Display ECU - Lane Assistant Active/Inactive	Controls the light that tells the driver if the Lane Departure Warning is activated
Car Display ECU - Lane Assistance malfunction warning	Controls the light that tells the driver if there is a malfunction
Driver Steering Torque Sensor	Responsible for measuring the torque provided by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Sense how much the driver is turning the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Block responsible for normal lane assistance item behavior
EPS ECU - Lane Departure Warning Safety Functionality	Responsible for guaranteeing functional safety requirements of the LDW function
EPS ECU - Lane Keeping Assistant Safety Functionality	Responsible for guaranteeing functional safety requirements of the LKA function
EPS ECU - Final Torque	Output final torque to the motor
Motor	Moves 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	50ms	LDW Safety Functionality	LDW torque output is set 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	50ms	LDW Safety Functionality	LDW torque output is set 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	50ms	LDW Safety Functionality	LDW torque output is set to zero

Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data Transmission Integrity Check	LDW torque output is set 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	Iginition cycle	Safety Startup	LDW torque output is set 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	The LDW safety component shall ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency’	C	50ms	LDW Safety Functionality	LDW torque output is set 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	50ms	LDW Safety Functionality	LDW torque output is set to zero
Technical Safety Requirement	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the	C	50ms	LDW Safety Functionality	LDW torque output is

03	'LDW_Torque_Request' shall be set to zero				set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured	C	50ms	Data Transmission Integrity Check	LDW torque output is set 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	Safety Startup	LDW torque output is set to zero

Lane Keeping Assistance (LKA) Requirements:

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

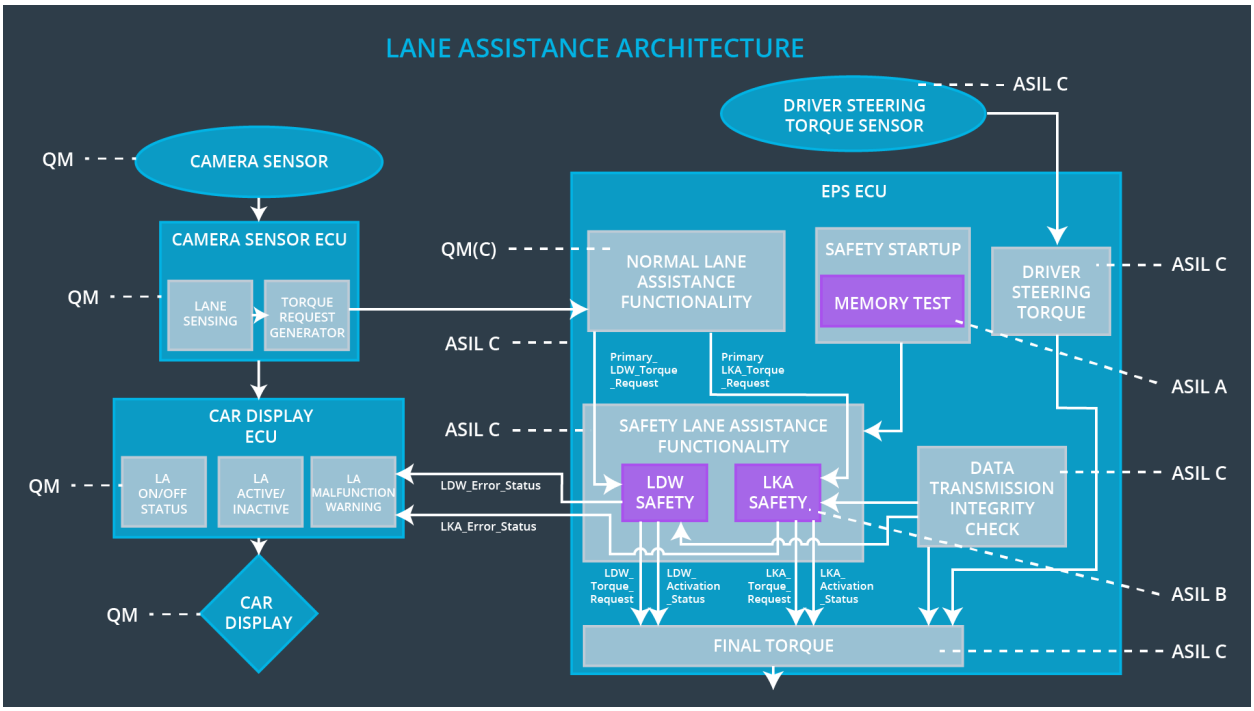
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**X**		

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 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is not active for a period longer than ‘Max_Duration’	B	500ms	LKA Safety Functionality	LKA torque output is set to zero
Technical Safety Requireme	As soon as the LKA function is turned off, the 'LKA Safety' software block shall send a signal	B	500ms	LKA Safety Functionality	LKA torque output is set to zero

nt 02	to the car display ECU to turn on a warning light				
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall turn off the lane keeping assistant and the 'LKA_Torque_Request' shall be set to zero	B	500ms	LKA Safety Functionality	LKA torque output is set 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	LKA torque output is set 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	Safety Startup	LKA torque output is set 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 the functionality	The lane departure warning function applies an oscillating torque with very high torque frequency or amplitude (above limit)	Yes	Warning light on the dashboard
WDC-02	Turn off the functionality	The lane keeping function torque is applied for a very long period (above limit)	Yes	Warning light on the dashboard