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
22/06/2018	1.0	Sameer Negi	Initial Draf

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept
- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

Technical Safety Concept
- Technical Safety Requirements
- Refinement of the System Architecture
- Allocation of Technical Safety Requirements to Architecture Elements
- Warning and Degradation Concept

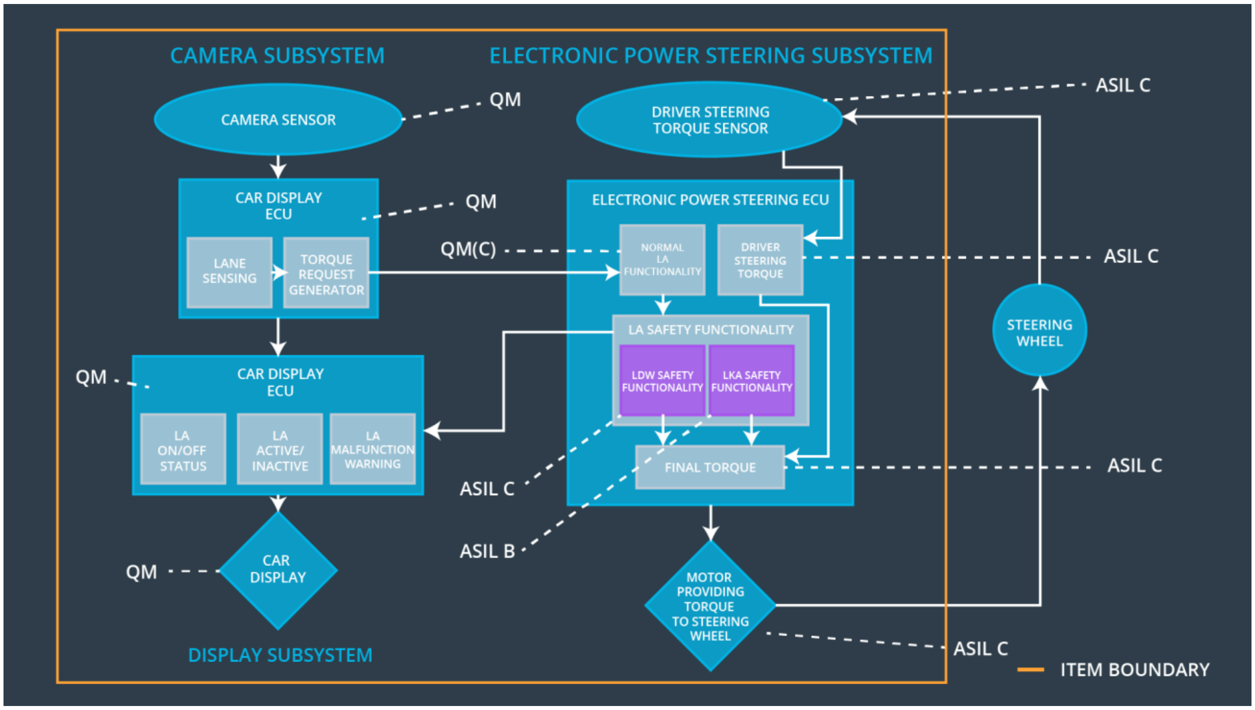
Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to specify the realization of the defined functional safety concept. 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	Turn off LDW
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Turn off LDW
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	Turn off LKA

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	A sensor for acquiring environment information as image.
Camera Sensor ECU - Lane Sensing	Software Module in the Camera Sensor ECU responsible for detecting lane lines and determining when the vehicle 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	Visual display responsible to displaying warning of lane departures and LKA and LDW activation and deactivations.
Car Display ECU - Lane Assistance On/Off Status	Visual display responsible to displaying LKA and LDW ON/OFF status.
Car Display ECU - Lane Assistant Active/Inactive	Visual display responsible to displaying displaying warning of lane departures, LKA and LDW

	activation and deactivations.
Car Display ECU - Lane Assistance malfunction warning	Visual display responsible to displaying warning of LKA and LDW malfunctions.
Driver Steering Torque Sensor	Sensor responsible for measuring how much force (steering torque) the driver is applying to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software Module in the electronic power steering ECU responsible for receiving the Camera Sensor ECU torque requests.
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_Fequency respectively.
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	Actuator responsible for applying requested torque to the steering column by the Electronic Power Steering ECU for either the LKA or the LDW functions.

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	LDW_Torque_Output= 0
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A
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	LDW_Torque_Output= 0
Technical Safety Requirement 04	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	LDW_Torque_Output= 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	Memory test	LDW_Torque_Output= 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	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	50 ms	LDW safety	LDW_Torque_Output = 0
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	N/A
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	LDW_Torque_Output = 0
Technical Safety	As soon as the LDW function	C	50 ms	LDW Safety	LDW_To

Requirement 04	deactivates the LDW feature, the 'LDW Safety' software block shall send a signal to the car display ECU to turn on a warning light.				rque_Output = 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	Memory test	LDW_Torque_Output= 0

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

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		

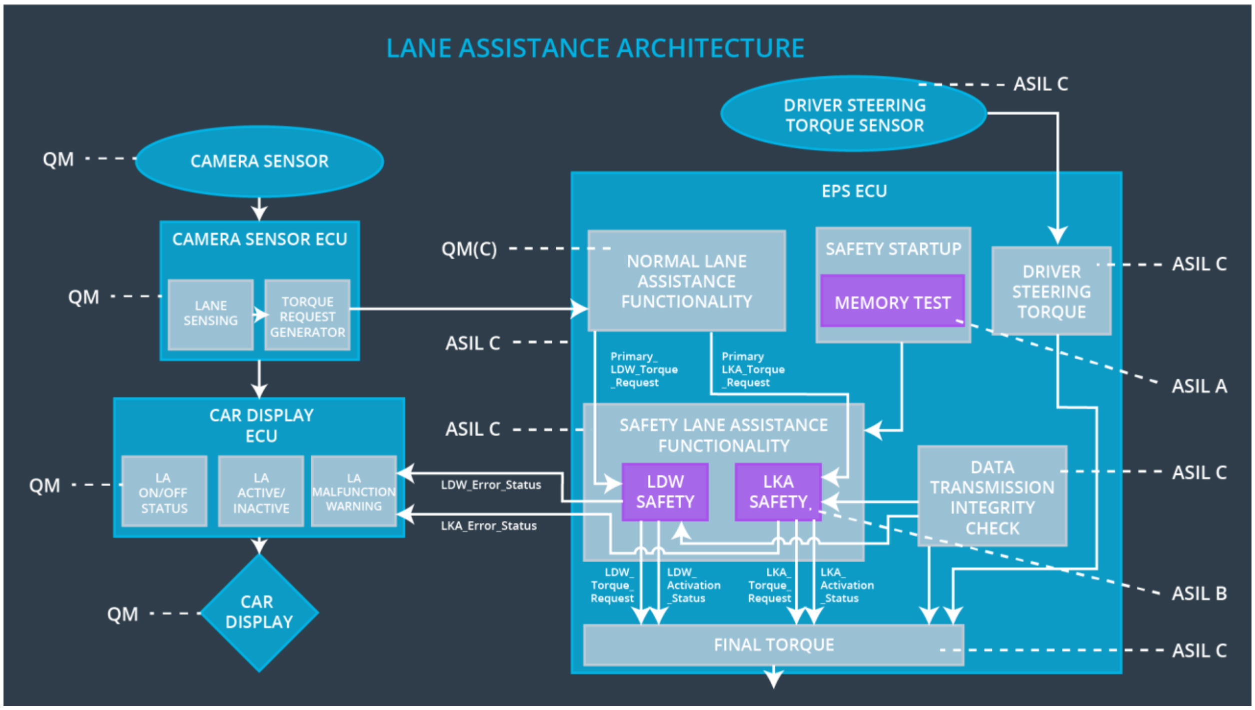
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 active duration time is below Max_Duration	B	500 ms	LKA safety	LKA_Torque _Output = 0
Technical Safety Requireme	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal	B	500 ms	Data Transmission Integrity Check	N/A

nt 02	shall be ensured				
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	500 ms	LKA safety	LKA_Torque _Output = 0
Technical Safety Requirement 04	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	LKA_Torque _Output = 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	500 ms	Memory Test	LKA_Torque _Output = 0

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

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

Based on the above tables, 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 function	Is_Max_Torque_Exceeded	Yes	Turn on warning light on car display
WDC-02	turn off the function	Is_Max_Duration_Exceeded	Yes	Turn on warning light on car display