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
12/24/2018	1.0	Melsobky	Initial Version
12/25/2018	1.1	Melsobky	Updated safe state for LDW & LKA

Table of Contents

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]

The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

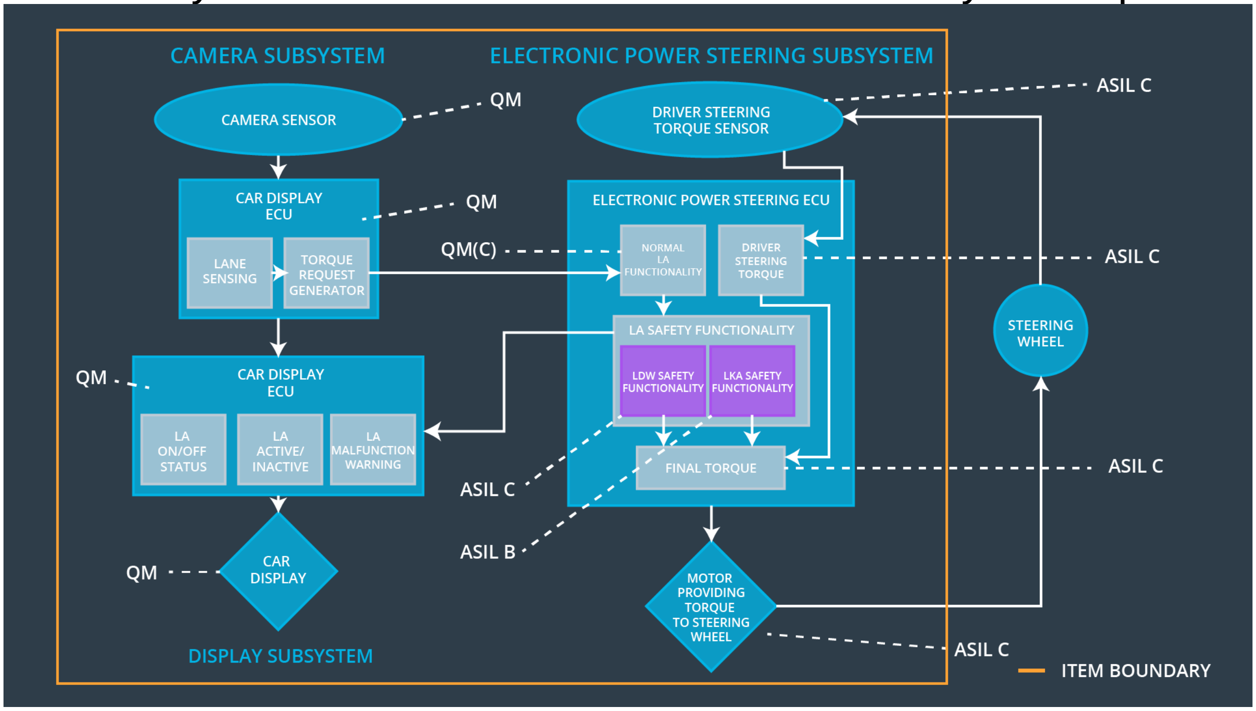
Inputs to the Technical Safety Concept

Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The EPS ECU shall ensure that the oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude	C	50 ms	LDW oscillating torque amplitude is set to 0
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	LDW oscillating torque amplitude is set to 0
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	LKA torque amplitude is set to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Provides camera images to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Detects laneline positions from camera images.
Camera Sensor ECU - Torque request generator	Generates a torque request to the Electronic Power Steering ECU.
Car Display	Shows warning and indications to driver.
Car Display ECU - Lane Assistance On/Off Status	Indicates the status of Lane Assistance functions (On / Off)
Car Display ECU - Lane Assistant Active/Inactive	Indicates the status of Lane Assistance functions (Active / Inactive)
Car Display ECU - Lane Assistance malfunction warning	Indicates malfunctions at LA functionality.

Driver Steering Torque Sensor	Reads the steering torque applied by the driver and send it to EPS ECU
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes input from Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Receives torque request from Camera Sensor ECU and transfers it to Safety Lane Assistance Functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Ensures that the torque amplitude is below Max_TorqueAmplitude and torque_frequency is below Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures that the LKA function is not active more than Max_duration time
EPS ECU - Final Torque	Generates final torque from torque requests received from LDW, LKA and driver.
Motor	Receives final torque calculated by Electronic Power Steering ECU and applies it to 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	A	Fault	Architecture	Safe State

	Requirement	**SIL**	**Tolerant Time Interval**	**Allocation**	
Technical Safety Requirement 01	The LDW safety component shall ensure that the *amplitude* of 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude'	C	50 ms	LDW Safety	LDW Torque *amplitude is set to 0*
Technical Safety Requirement 02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the 'LDW_Torque_Request' shall e set to zero	C	50 ms	LDW Safety	LDW Torque *amplitude is set to 0*
Technical Safety Requirement 03	As soons 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 *amplitude is set to 0*
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	LDW Torque *amplitude is set to 0*
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory.	A	ignition cycle	Memory Test	LDW Torque *amplitude is set to 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	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 *frequency* of ‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency’	C	50 ms	LDW Safety	LDW Torque *amplitude is set to 0*
Technical Safety Requirement 02	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ‘LDW_Torque_Request’ shall e set to zero.	C	50 ms	LDW Safety	LDW Torque *amplitude is set to 0*
Technical Safety Requirement 03	As soons 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 *amplitude is set to 0*
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	LDW Torque *amplitude is set to 0*
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory	A	ignition cycle	Memory Test	LDW Torque *amplitude is set to 0*

Lane Keeping Assistance (LKA) Requirements:

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

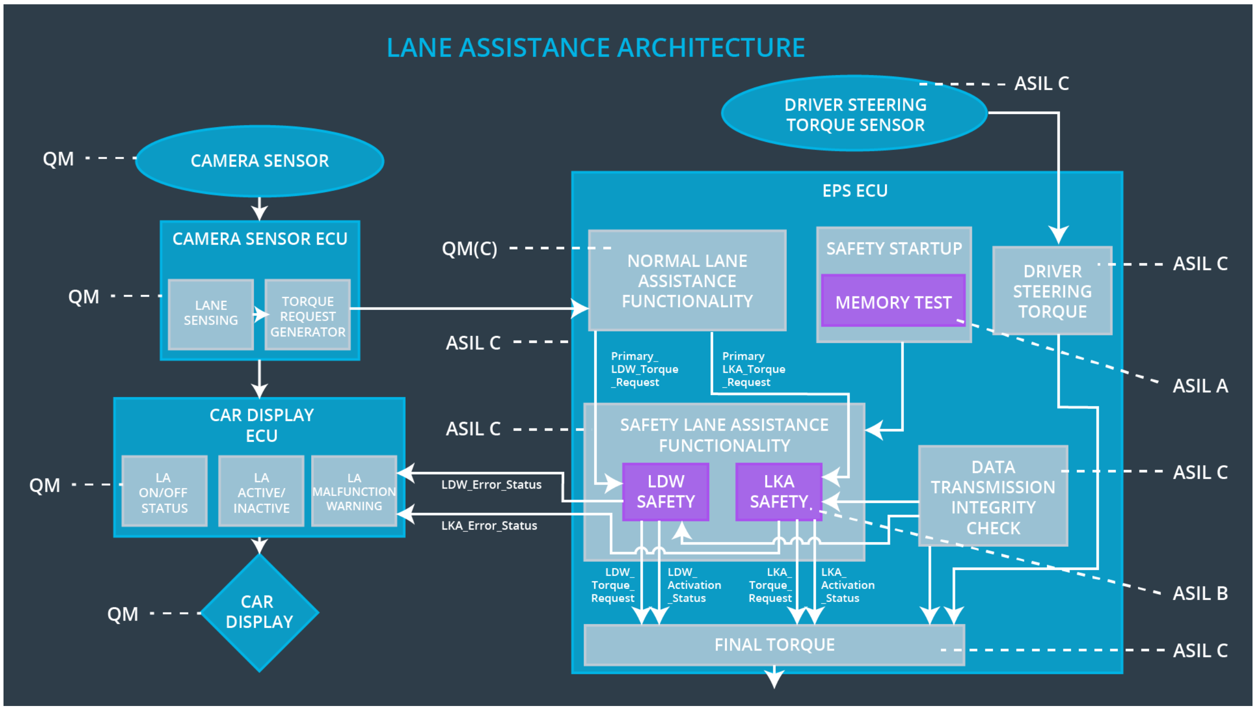
ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 ‘LKA_Torque_Request’ is sent to the ‘Final electronic power steering Torque’ component for only ‘Max_Duration’.	B	500 ms	LKA Safety	*LKA Torque amplitude is set to 0*
Technical Safety Requirement 02	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ‘LKA_Torque_Request’ shall e set to zero.	B	500 ms	LKA Safety	*LKA Torque amplitude is set to 0*
Technical Safety Requirement 03	As soons 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 amplitude is set to 0*

Technical Safety Requireme nt 04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	*LKA Torque amplitude is set to 0*
Technical Safety Requireme nt 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in mermory.	A	ignition cycle	Memory Test	*LKA Torque amplitude is set to 0*

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	*LDW Torque amplitude is set to 0*	Malfunction_01, Malfunction_02	Yes	LDW malfunction warning on Dar Display
WDC-02	*LKA Torque amplitude is set to 0*	Malfunction_03	Yes	LKA malfunction warning on Dar Display