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
2019-01-23	1.0		First draft

Table of Contents

Table of Contents

Purpose of the Technical Safety Concept

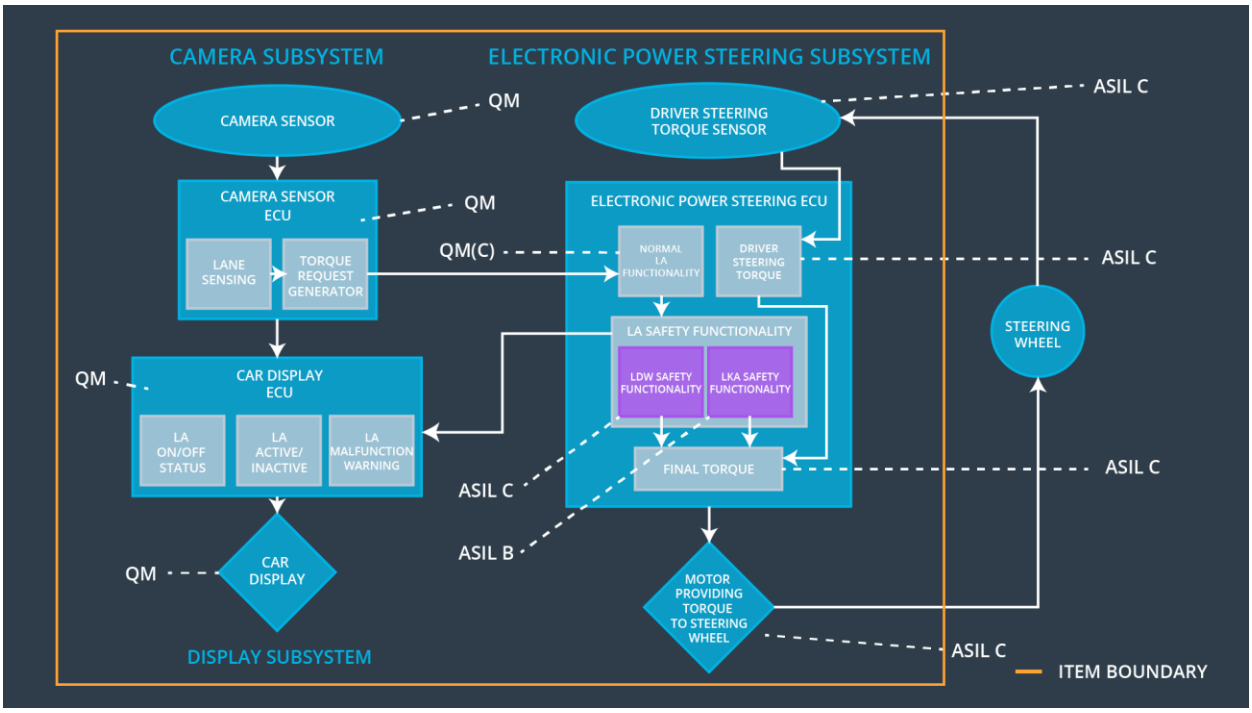
The purpose of the technical safety concept is, to add more technical details to the functional safety concept. Create new requirements and allocate them to the system architecture.

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	OFF
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	OFF
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	OFF

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Records an image of the current road
Camera Sensor ECU - Lane Sensing	Calculates the position and orientation of the car respectively to the lane lines
Camera Sensor ECU - Torque request generator	Calculates the torque to be applied to the steering wheel in order to get back to the center of the lane
Car Display	Displays the status of the functions and the driver warnings
Car Display ECU - Lane Assistance On/Off Status	Controls the LED for the status
Car Display ECU - Lane Assistant Active/Inactive	Controls the LED for the status
Car Display ECU - Lane Assistance malfunction warning	Controls the LED for the warning
Driver Steering Torque Sensor	Senses the torque the driver applies to the steering wheel

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads the Driver Steering Torque Sensor and passes the driver steering torque to the Final Torque unit
EPS ECU - Normal Lane Assistance Functionality	Receives the torque request from the Camera Sensor ECU and passes it to the LA Safety Functionality. It also limits the torque request in amplitude and frequency.
EPS ECU - Lane Departure Warning Safety Functionality	It deactivates the LDW if the torque request amplitude or frequency exceeds the limits
EPS ECU - Lane Keeping Assistant Safety Functionality	It deactivates the LKA if the driver does not steer the car anymore for the maximum amount of time
EPS ECU - Final Torque	Combines the LDW, LKA and the driver steering torque requests to the final torque, which will be used for the steering motor
Motor	Applies the torque 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	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 the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Amplitude'.	C	50 ms	LDW Safety block	LDW torque output is set to zero
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 block	LDW torque output is set to zero
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 block, LA malfunction warning block	LDW torque output is set 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	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	50 ms	LDW Safety block	OFF
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, LA malfunction warning block	OFF
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	OFF
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	OFF
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	OFF

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		

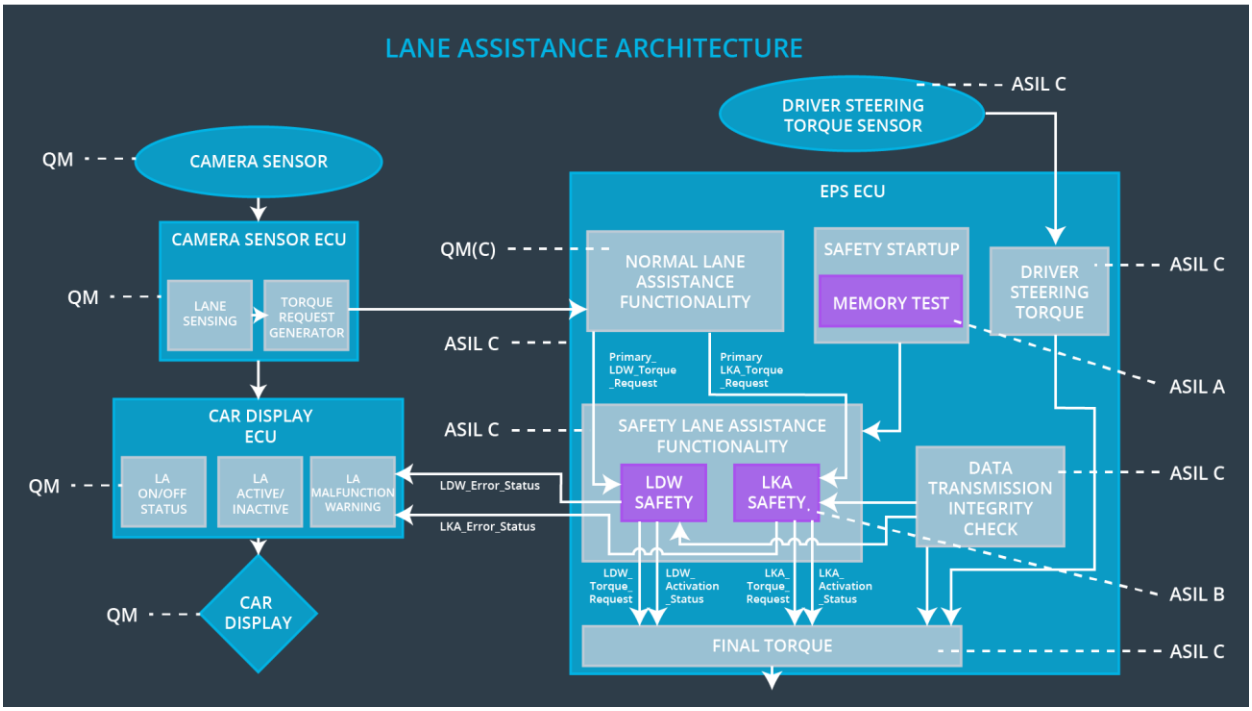
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

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 lane keeping assistance torque is applied for only 'Max_Duration'.	B	500 ms	LKA Safety block	OFF
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	500 ms	LKA Safety block, LA malfunction warning block	OFF
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 block	OFF
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	OFF

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	OFF

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

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For the lane keeping item all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation	Safe State invoked?	Driver Warning

		Mode		
WDC-01	OFF	LDW torque or frequency limit exceeded	YES	Display message and turn on a warning light
WDC-02	OFF	LKA driver hands not at steering wheel	YES	Display message and turn on a warning light