Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
6/25/18	1.0	Pascal Irminger	Technical Safety Concept (init)
6/28/18	1.1	Pascal Irminger	Safe State Refinement

Table of Contents

Purpose of the Technical Safety Concept

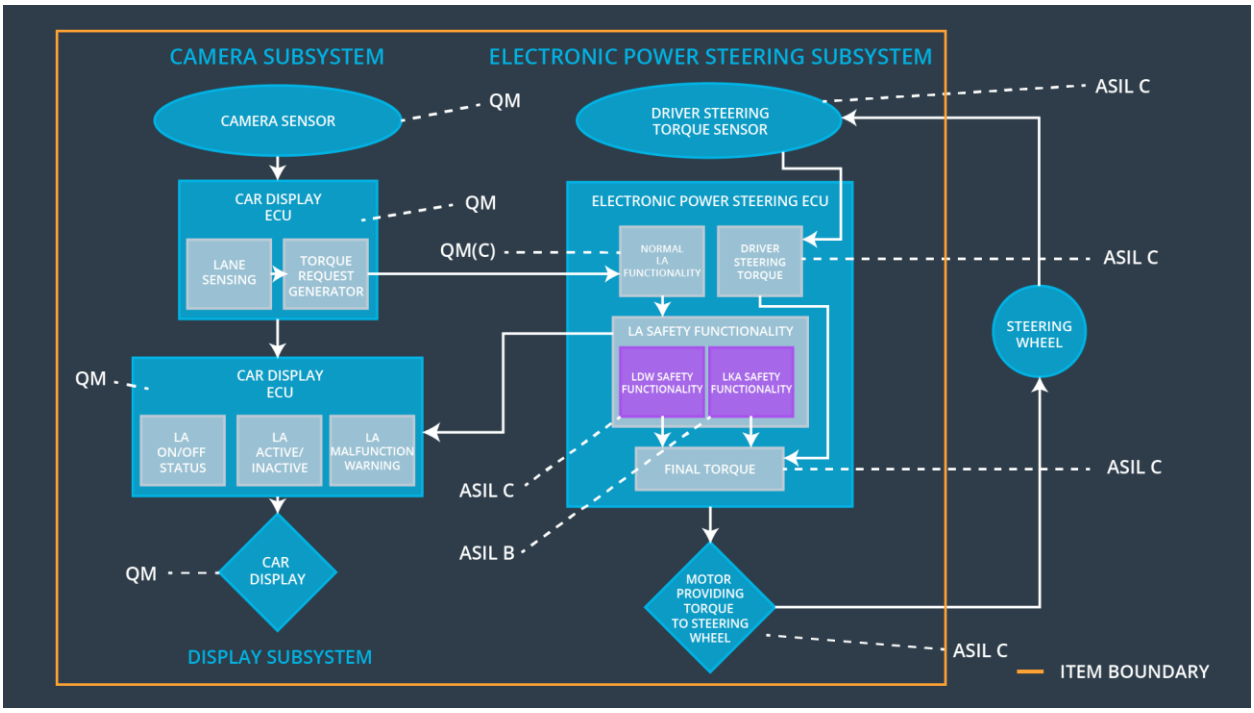
The Technical Safety Concept document refines the functional safety requirements established in the Functional Safety Concept into technical safety requirements and assigns them to the system architecture.

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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Oscillation torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Oscillation torque frequency below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The electronic power steering ECU shall ensure that the lane departure oscillating torque is zero if Lane_Not_Found is stated true by the camera sensor ECU.	B	10 ms	LDW function is turned 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	500 ms	LKA torque is zero.
Functional Safety Requirement 02-02	The electronic power steering ECU shall not request torque if Lane_Is_Yellow is stated true by the camera sensor ECU.	A	25 ms	LKA function is turned off.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures road images and provides them to the Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Software module detecting lane line positions from the Camera Sensor images.
Camera Sensor ECU - Torque request generator	Software module calculating the necessary torque to be requested to the Electronic Power Steering (EPS) ECU.
Car Display	Provides feedback to the driver by displaying warnings and the LDA function status.
Car Display ECU - Lane Assistance On/Off Status	Indicates the status of the Lane Assistance functionality (On/Off).
Car Display ECU - Lane Assistant Active/Inactive	Indicates the status of the Lane Assistance functionality (Active/Inactive).

Element	Description
Car Display ECU - Lane Assistance malfunction warning	Indicates a malfunction of the Lane Assistance functionality.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module receiving the torque request from the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Software module receiving the torque request from the Camera Sensor ECU.
EPS ECU - Lane Departure Warning Safety Functionality	Software module ensuring the LDW function torque amplitude is below Max_Torque_Amplitude and the torque frequency is below Max_Torque_Frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module ensuring the LKA function is not activate more than Max_Duration.
EPS ECU - Final Torque	Software module combining the torque requests from the LDW function and the LKA function and sending the final torque to the steering wheels.
Motor	Applies the torque indicated by the Electronic Power Steering ECU 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 01-01-01	The LDW safety component shall ensure that the amplitude of the ‚LDW_Torque_Request' sent to the ‚Final EPS Torque' component is below ‚Max_Torque_Amplitude'.	C	50 ms	LDW Safety	LDW Torque Request Amplitude is zero.
Technical Safety Requirement 01-01-02	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 Request Amplitude is zero.
Technical Safety Requirement 01-01-03	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 Request Amplitude is zero.
Technical Safety Requirement 01-01-04	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 Request Amplitude is zero.
Technical Safety Requirement 01-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Length of vehicle ignition cycle	Memory Test	LDW Torque Request Amplitude is zero.

Functional Safety Requirement 01-02 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 01-02-01	The LDW safety component shall ensure that the frequency of the ‚LDW_Torque_Request' sent to the ‚Final EPS Torque' component is below ‚Max_Torque_Frequency'.	C	50 ms	LDW Safety	LDW Torque Request Frequency is zero.

Lane Keeping Assistance (LKA) Requirements:

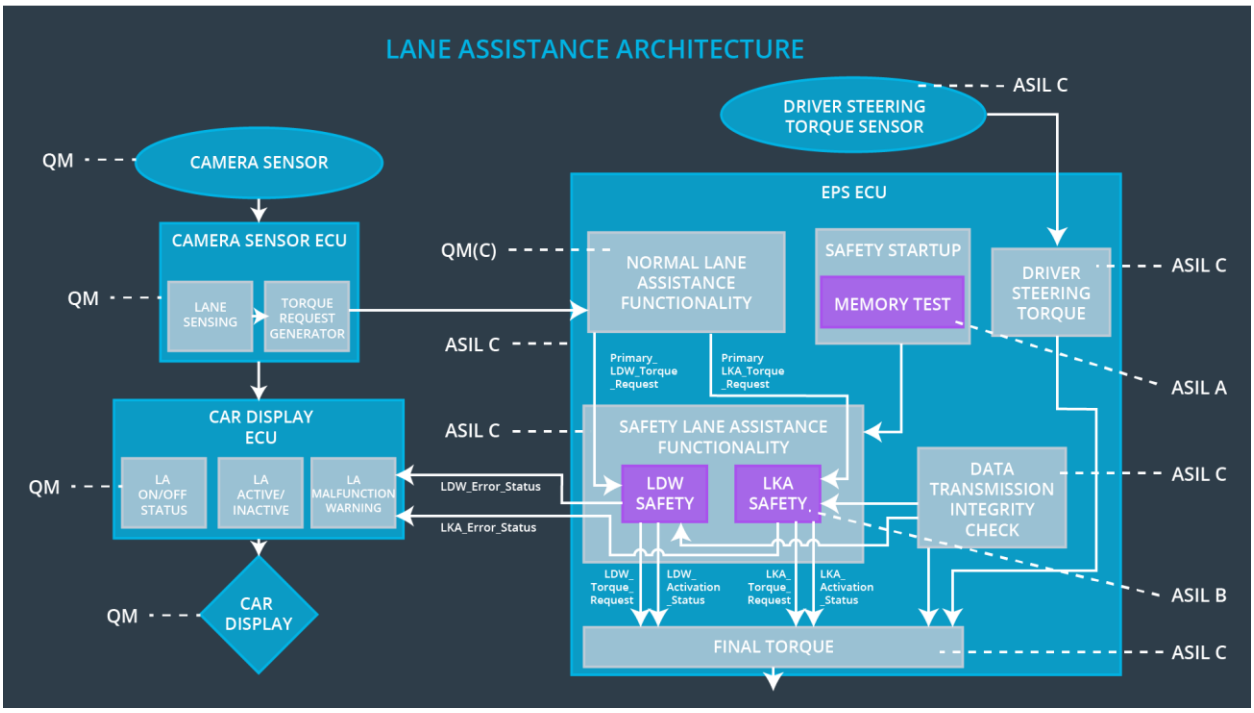
Functional Safety Requirement 02-01 with its associated system elements
(derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 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 02-01-01	The LKA safety component shall ensure that the duration of the lane keeping assistance torque is applied for less than ‚Max_Duration‘.	B	500 ms	LKA Safety	LKA torque is zero.
Technical Safety Requirement 02-01-02	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.	C	50 ms	LKA Safety	LKA torque is zero.
Technical Safety Requirement 02-01-03	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.	C	50 ms	LKA Safety	LKA torque is zero.
Technical Safety Requirement 02-01-04	The validity and integrity of the data transmission for ‚LKA_Torque_Request‘ signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	LKA torque is zero.
Technical Safety Requirement 02-01-05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Length of vehicle ignition cycle	Memory Test	LKA torque is zero.

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements are allocated to the Electronic Power Steering (EPS) ECU. For the exact allocation within EPS ECU compare the technical safety requirement tables above.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function	Malfunction_01, Malfunction_02, Malfunction_03	Yes	LDW malfunction warning on car display
WDC-02	Turn off LKA function	Malfunction_04, Malfunction_05	Yes	LKA malfunction warning on car display