Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 3.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
18.03.2018	1.0	P. Schalast	Initial commit
31.03.2018	2.0	P. Schalast	Review for project commit
02.04.2018	3.0	P. Schalast	Minor changes

Table of Contents

Purpose of the Technical Safety Concept

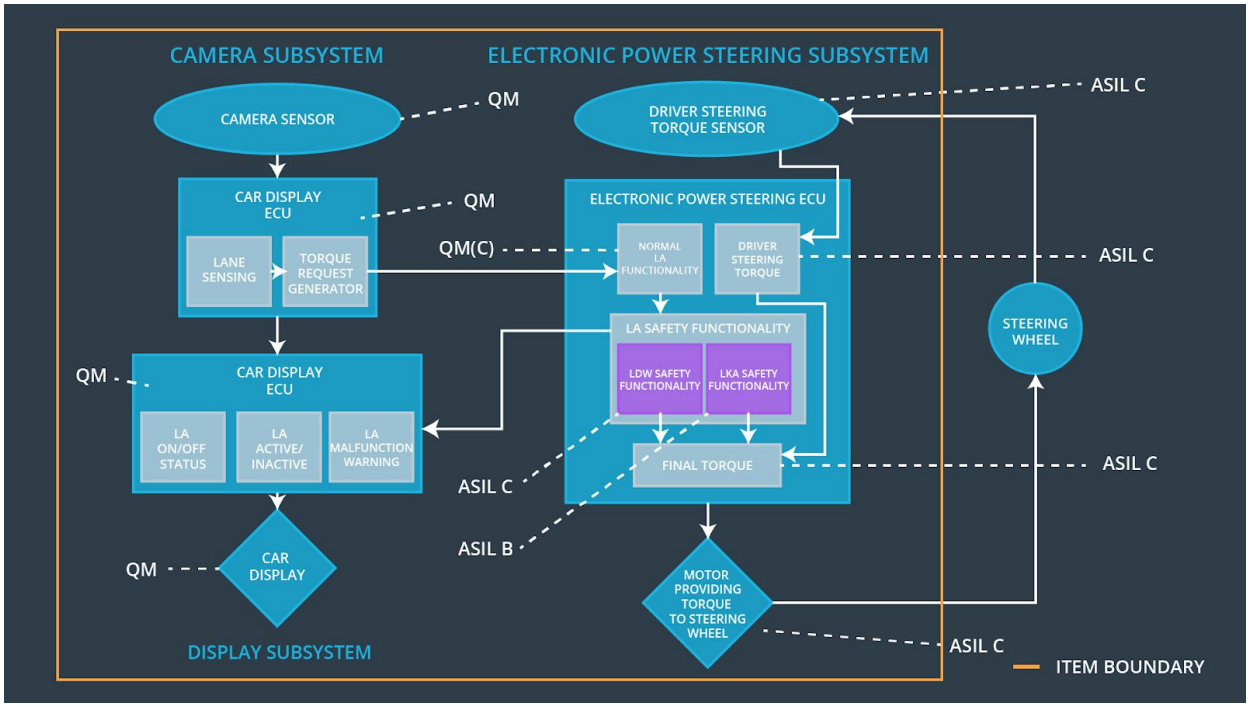
ISO 26262 places the functional safety concept in the concept phase while the technical safety concept is part of the product development phase.
This is because the technical safety concept is more concrete and gets into the details of the item's technology. The product development phase also includes designing hardware and software. This lesson will only focus on the technical safety concept, and the next lesson will discuss hardware and software development.

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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Gradually reduce steering torque to 0
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Gradually reduce steering torque to 0
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	Gradually reduce steering torque to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Capture images from the road ahead and provide to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detect lane lines in the received images, derive position and direction of the vehicle relative to the lanes
Camera Sensor ECU - Torque request generator	Calculate correction torque request
Car Display	Display warnings and information
Car Display ECU - Lane Assistance On/Off Status	Indicate status of the Lane Assistance system (on/off)
Car Display ECU - Lane Assistant Active/Inactive	Indicate current functionality of the Lane Assistance system (active/inactive)

Car Display ECU - Lane Assistance malfunction warning	Indicate a malfunction of the Lane Assistance system
Driver Steering Torque Sensor	Measure torque set by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receiving the drivers torque request from the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Receiving torque request from the Camera Sensor ECU
EPS ECU - Lane Departure Warning Safety Functionality	Safety module to ensure that torque amplitude and frequency are below its maximum
EPS ECU - Lane Keeping Assistant Safety Functionality	Safety module to ensure LKA is not activated longer than maximum duration time
EPS ECU - Final Torque	Combine torque requests from LKA and LDW to final torque request to be send to the motor
Motor	Apply final torque for vehicle steering

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_Request set to 0
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	LDW_Torque_Request set to 0

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_Request 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_Request 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 memory.	A	Ignition cycle	Safety Startup	LDW_Torque_Request 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 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_Request set to 0
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	LDW_Torque_Request set to 0
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_Request 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_Request 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 memory.	A	Ignition cycle	Safety Startup	LDW_Torque_Request set to 0

Lane Keeping Assistance (LKA) Requirements:

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

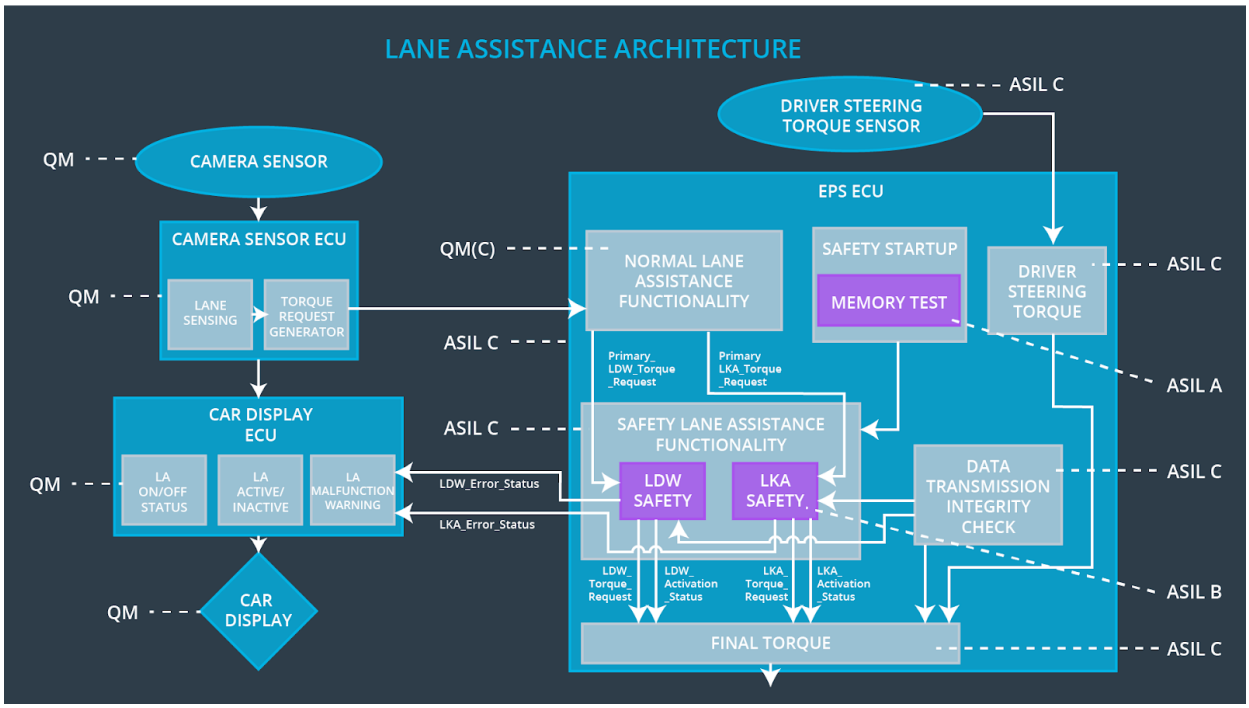
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 the duration of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below Max_Duration.	B	500 ms	LKA_Safety	LKA_Torque_Request set to 0
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	LKA_Torque_Request set to 0
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_Request set to 0
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	LKA_Torque_Request 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 memory.	A	Ignition cycle	Safety Startup	LKA_Torque_Request 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_Request set to 0	Torque above limit	Yes	Warning via car display
WDC-02	LKA_Torque_Request set to 0	Time limit exceeded	Yes	Warning via car display