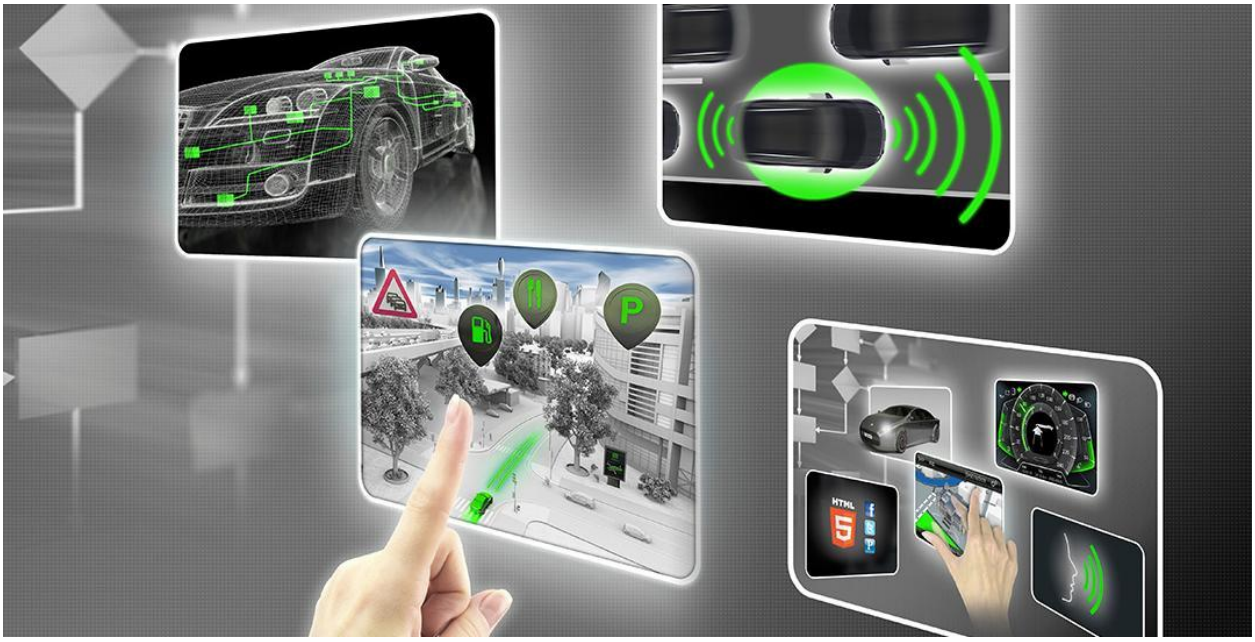
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0



Document history

Date	Version	Editor	Description
15.08.2018	1.0	Reuss	First version

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the Technical Safety Concept is to:

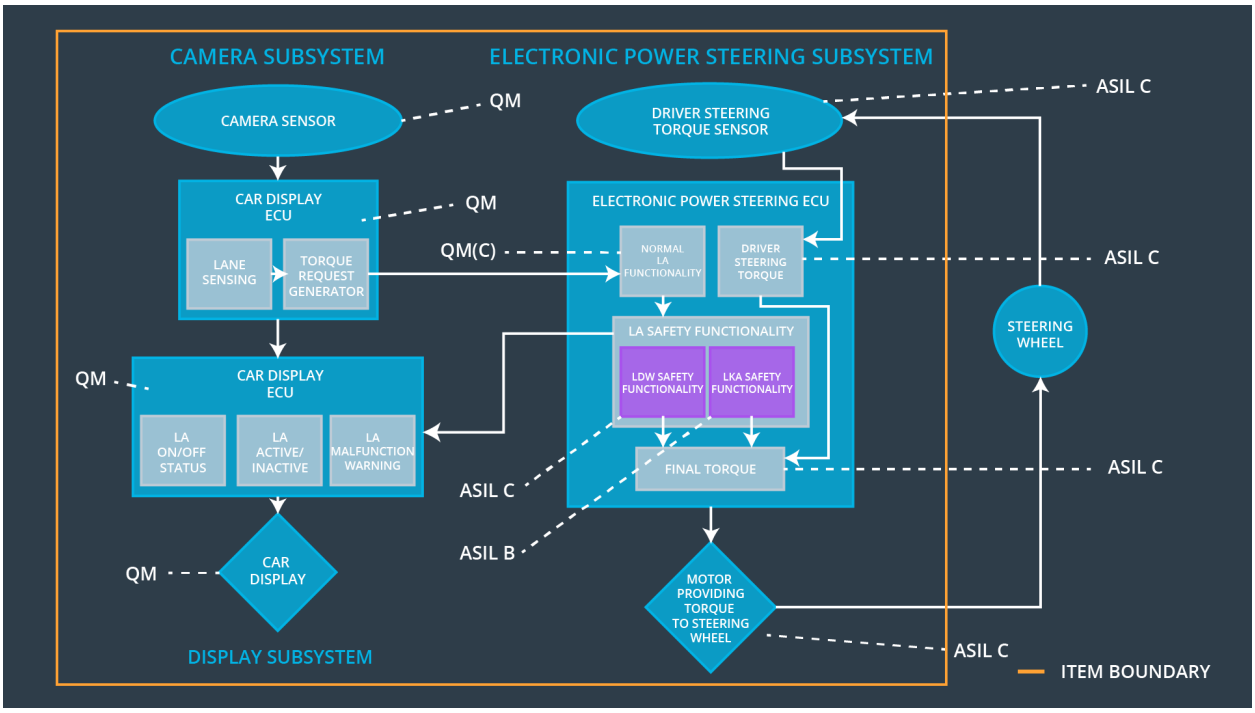
- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

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 oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Set vibration torque to zero and shut off system
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	50ms	Set vibration torque to zero and shut off system
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	Shut off system

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Takes images of the road.
Camera Sensor ECU - Lane Sensing	Processes images taken by the camera sensor and identifies lanes.
Camera Sensor ECU - Torque request generator	Processes identified lanes together with the cars position and generates a torque request, that is sent to the Electronic power steering ECU.
Car Display	Display used to share information with the driver.
Car Display ECU - Lane Assistance On/Off Status	Symbol in vehicle display that tells the driver if the lane assistance system is in status On/Off.
Car Display ECU - Lane Assistant Active/Inactive	Symbol in vehicle display that tells the driver if the lane assistance system is in status Active/Inactive.
Car Display ECU - Lane Assistance malfunction warning	Symbol in vehicle display that warns the driver if the lane assistance system malfunctions.
Driver Steering Torque Sensor	Measures torque applied by the driver the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes inputs of driver steering torque sensor.
EPS ECU - Normal Lane Assistance Functionality	Software block that processes torque request input from camera sensor ECU and outputs a torque request to both safety software blocks LDW safety functionality and LKA safety functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Safety software block that validates the requested torque by the normal lane assistance functionality regarding amplitude and frequency. Generates a torque request as output.
EPS ECU - Lane Keeping Assistant Safety Functionality	Safety software block that validates the requested torque by the normal lane assistance functionality regarding duration of lane keep assistance functionality switched on. Generates a torque request as output.
EPS ECU - Final Torque	Resulting final torque request sent to the motor.
Motor	Adds additional torque to the steering wheel, if requested.

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	50ms	LDW Safety block	Lane Departure Warning Torque shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity check	Lane Departure Warning Torque shall be set to zero
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	50ms	LDW Safety block	Lane Departure Warning Torque shall be 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	50ms	LDW Safety block	Lane Departure Warning Torque shall be set to zero
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	Lane Departure Warning Torque shall be 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency'.	C	50ms	LDW Safety block	Lane Departure Warning Torque shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity check	Lane Departure Warning Torque shall be set to zero

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	50ms	LDW Safety block	Lane Departure Warning Torque shall be 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	50ms	LDW Safety block	Lane Departure Warning Torque shall be set to zero
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	Lane Departure Warning Torque shall be set to zero

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:

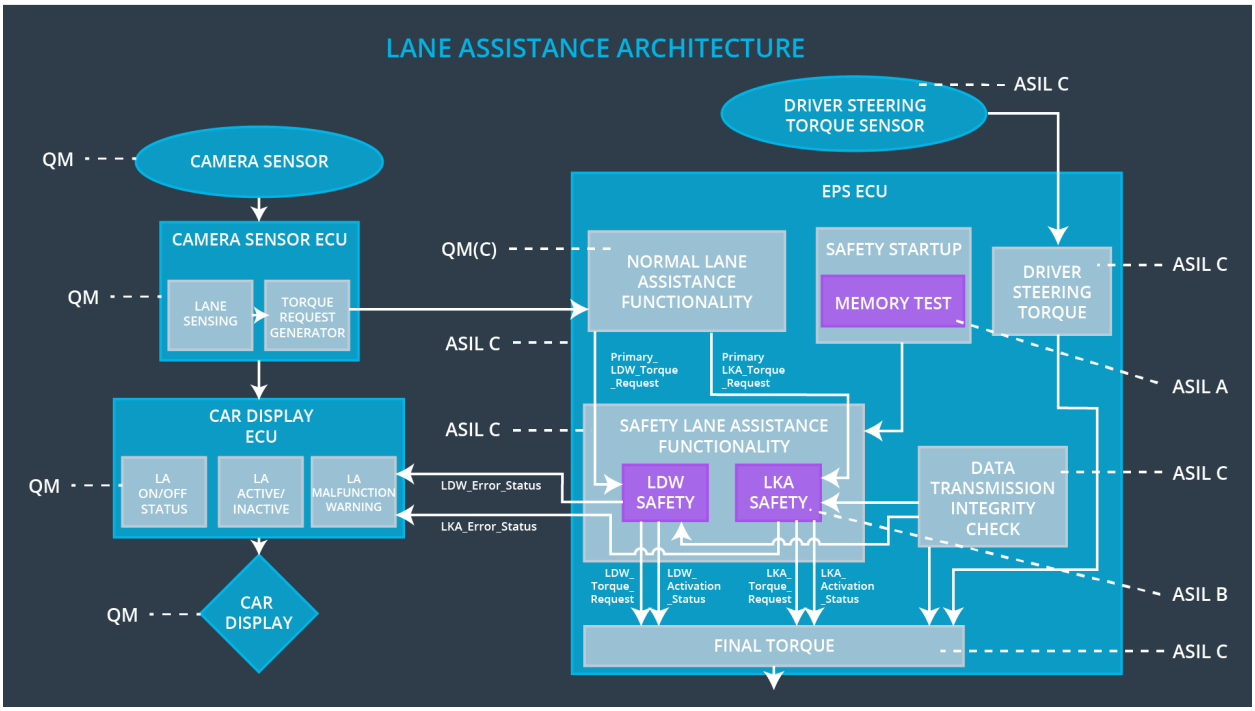
ID	Technical Safety Requirement	A S	Fault Tolerant	Allocation to Architecture	Safe State

		IL	Time Interval		
Technical Safety Requirement 01	The LKA safety component shall ensure that the time of sending 'LKA_Torque_Request' to the 'Final electronic power steering Torque' component is below 'Max_Duration'.	B	500ms	LKA Safety block	Lane Keep Assistance Torque shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity check	Lane Keep Assistance Torque shall be set to zero
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	500ms	LKA Safety block	Lane Keep Assistance Torque shall be set to zero
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	500ms	LKA Safety block	Lane Keep Assistance Torque shall be set to zero
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	Lane Keep Assistance Torque shall be set to zero

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

...

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	Turn off functionality	Torque amplitude over Max_Torque_Amplitude OR Torque frequency over Max_Torque_Frequency	Yes	Play alarm sound. Display warning “Lane assistance system is shut off due to malfunction.”
WDC-02	Turn off functionality	Driver did not put hands on the steering wheel for time longer than Max_Duration	Yes	Display warning “Lane assistance system is not designed for autonomous driving. Driver is responsible to control the car at all times. System is shut off.”