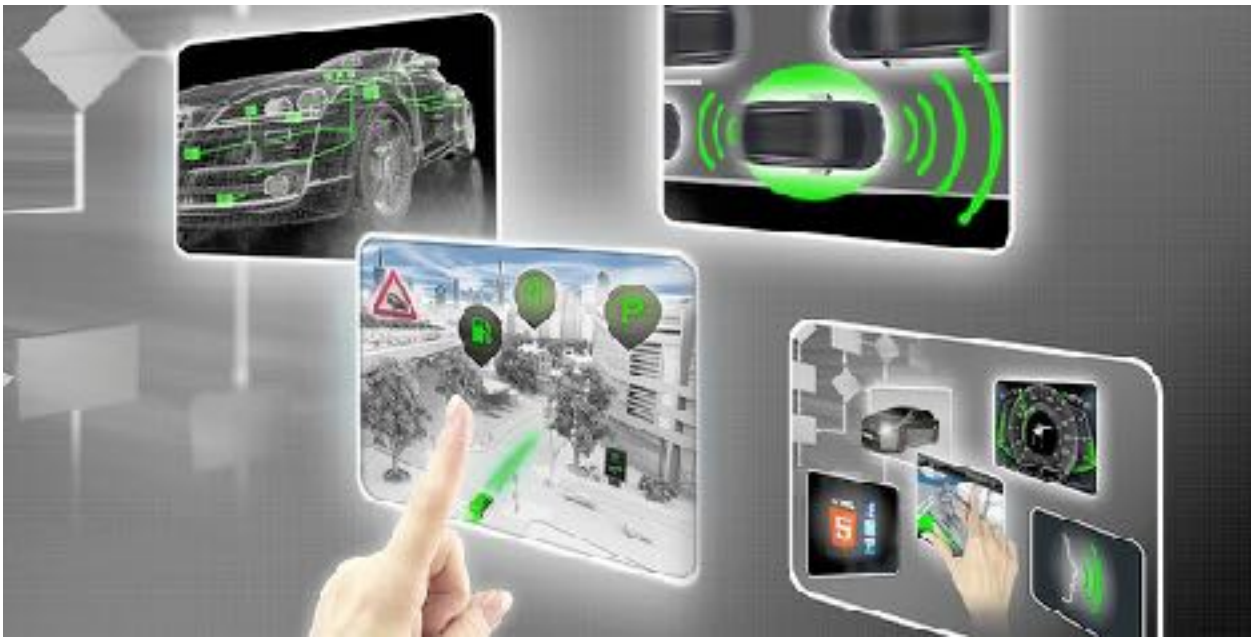
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2/27-28/2018	1.0	Mark Veronda	Filling out Document while following class

Table of Contents

Purpose of the Technical Safety Concept

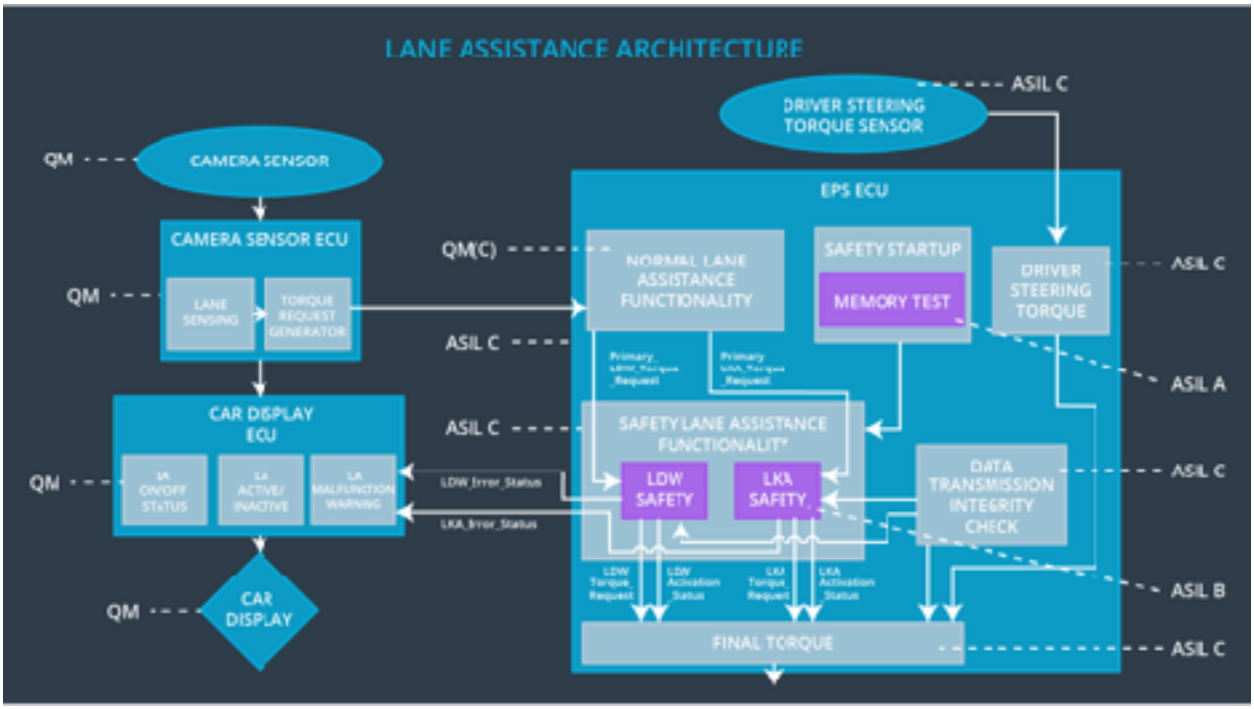
The purpose of the technical safety concept is to pick up the next phase of ISO-26262 design and development and precisely define how all the subsystems will communicate with each other. Whereas previously we made a functional safety document, that was at the end of the "design" side of the V (to the left), and the technical safety is now moving us back up the implementation and testing side of the V (to the right). It also brings things down to a lower-level, whereas the functional safety concept can be considered the "birds-eye" or "20,000 ft" view.

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	The LDW turns off to stop applying the amplitude
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	The LDW turns off to stop applying the amplitude
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the LKA torque is applied for only Max_Duration.	C	500ms	The LKA should turn off and the driving remain in control of car.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Detecting lane lines and car's position in relation to ego lane
Camera Sensor ECU - Lane Sensing	Detecting when lane departure is occurring
Camera Sensor ECU - Torque request generator	Send amplitude and frequency torque oscillation command to Power Steering ECU to vibrate the wheel.
Car Display	Displays to driver lane-departure warning sign
Car Display ECU - Lane Assistance On/ Off Status	Responsible for informing driver whether the LKA is on or off
Car Display ECU - Lane Assistant Active/Inactive	Responsible for informing driver whether the LKA is currently applying torque to the wheel or is not
Car Display ECU - Lane Assistance malfunction warning	Responsible for informing driver that the LKA has malfunctioned.
Driver Steering Torque Sensor	Detects driver’s input to the wheel (and lack of)

Element	Description
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Responsible for sending torque requests to the EPS
EPS ECU - Normal Lane Assistance Functionality	This should just keep torque at zero until the camera informs this system that car has drifted from ego lane.
EPS ECU - Lane Departure Warning Safety Functionality	This should receive request to change torque from the LDW safety to vibrate wheel
EPS ECU - Lane Keeping Assistant Safety Functionality	Receives torque requests from LKA to keep car inside the ego lane.
EPS ECU - Final Torque	The final torque to send to the EPS, ensuring it is well within safety parameters
Motor	Taking input from Electronic Power Steering ECU to apply the requested torque change (and safely, within limits)

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:

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
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 block	LDW_Torque_ Request Amplitude shall be set to zero
02	As soon as LDW deactivates the 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	LDW_Torque_ Request Amplitude shall be set to zero
03	As soon as a failure is detected by the LDW, it shall deactivate the feature and the ‘LDW_Torque_Request’ shall be set to zero	C	50 ms	LDW Safety block	LDW_Torque_ Request Amplitude shall be set to zero
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 shall be set to zero
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 Memory Test	LDW_Torque_ Request Amplitude 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:

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
01	The LDW safety component shall ensure that the frequency of the ‘LDW_Torque_Request’ sent to the ‘Final EPS Frequency’ component is below ‘Max_Torque_Frequency’.	C	50 ms	LDW Safety block	LDW_Torque_Request Frequency shall be set to zero
02	As soon as LDW deactivates the 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	LDW_Torque_Request Frequency shall be set to zero
03	As soon as a failure is detected by the LDW, it shall deactivate the feature and the ‘LDW_Torque_Request’ shall be set to zero	C	50 ms	LDW Safety block	LDW_Torque_Request Frequency shall be set to zero
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 Frequency shall be set to zero
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 Memory Test	LDW_Torque_Request Frequency shall be set to zero

Lane Keeping Assistance (LKA) Requirements:

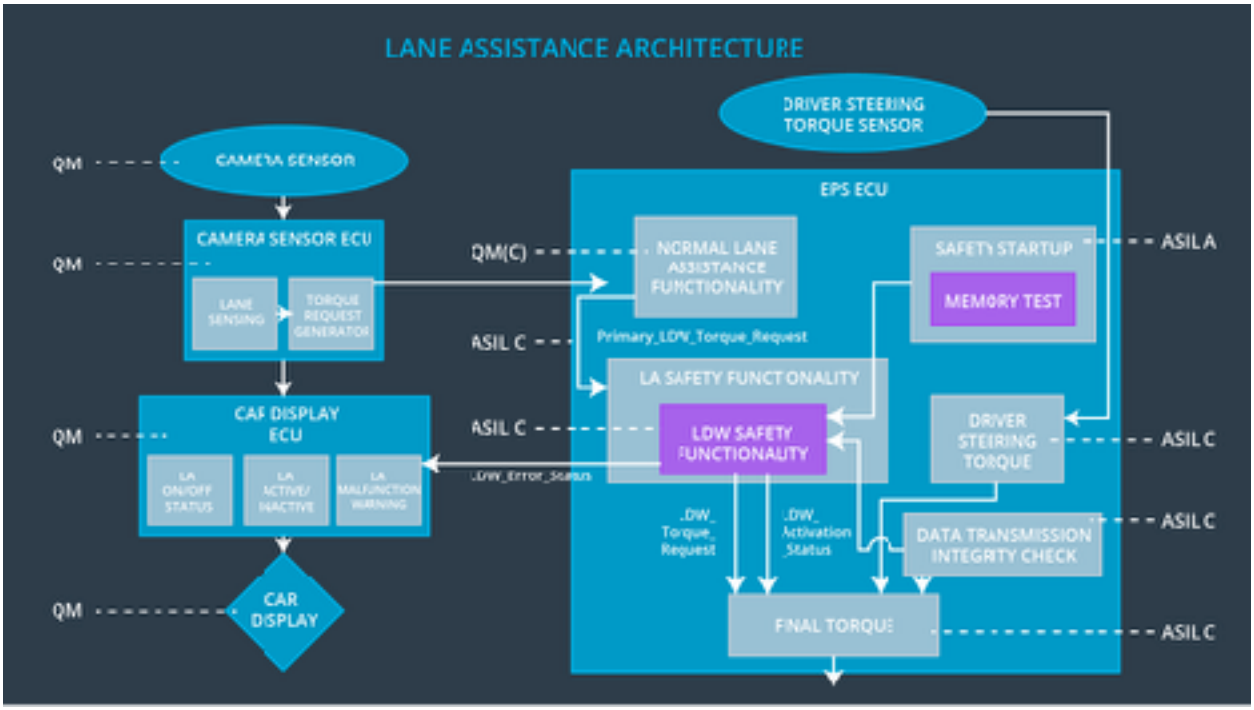
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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:

Technical Safety Req. ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
01	The LKA safety component shall ensure that the duration of the 'LKA_Torque_Request' sent to the 'Final EPS Torque' is for less than 'Max_Duration'.	B	500 ms	LKA Safety Block	LKA_Torque_Request shall be set to zero
02	As soon as LKA deactivates the 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	LKA_Torque_Request shall be set to zero
03	As soon as a failure is detected by the LKA, it shall deactivate the feature and the 'LKA_Torque_Request' shall be set to zero	B	500 ms	LKA Safety Block	LKA_Torque_Request shall be set to zero
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 shall be set to zero
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 Memory Test	LKA_Torque_Request shall be set to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

Allocation can already be found in the tables above. 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	Shut down LDW functionality	Steering wheel oscillation frequency or amplitude exceeds parameters	Yes	Warning icon displayed on Dashboard
WDC-02	Shut down LKA functionality	LKA functionality applies torque for longer than max_duration.	Yes	Warning icon displayed on Dashboard