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
2018/06/10	1.0	Frank . W	First Version

Table of Contents

Purpose of the Technical Safety Concept

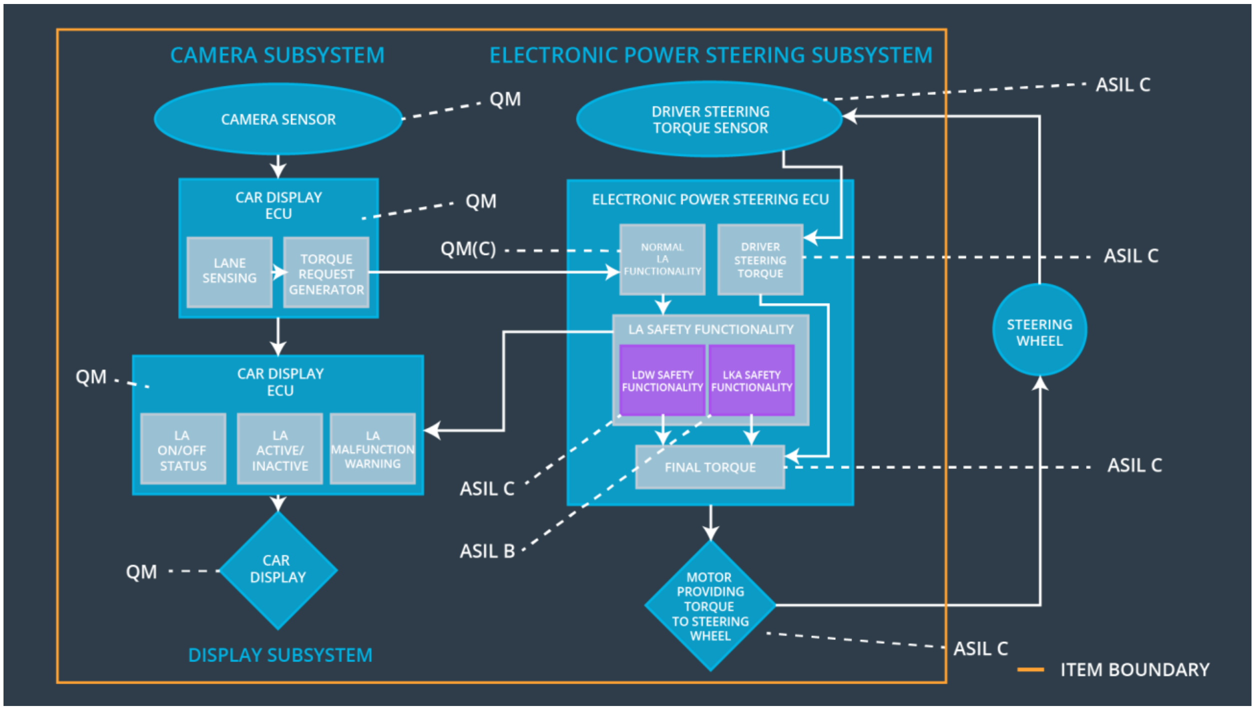
Given the functional safety requirements, deriving technical safety requirements based on system architecture, determining the property of technical safety requirements such as ASIL, fault tolerant time interval, and safe state as well as verification and validation acceptance criteria, then refining the system architecture and allocating requirements, finally, defining warning and degradation concept.

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 amplitude 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	50ms	Set vibration torque frequency 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	500ms	Set lane keeping assistance torque to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Transform ambient information into digital images and send them to Camera Sensor ECU.
Camera Sensor ECU - Lane Sensing	Detect lane line from digital images send by Camera Sensor.
Camera Sensor ECU - Torque request generator	Calculate the vehicle position in lane, and generate torque request to EPS.
Car Display	Transform the information sent by Car Display ECU into visual signals
Car Display ECU - Lane Assistance On/Off Status	Collect Lane Assistance On/Off status information and show the information to the driver by controlling Car Display.
Car Display ECU - Lane Assistant Active/Inactive	Collect Lane Assistance Active/Inactive status information and show the information to the driver by controlling Car Display.
Car Display ECU - Lane Assistance malfunction warning	Collect Lane Assistance malfunction warning information and show the information to the driver by controlling Car Display.
Driver Steering Torque Sensor	Transform the Steering Torque into electrical signal
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Calculate the turning direction and torque of the motor according to the steering direction and torque size sent by the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Apply an oscillating steering torque to provide the driver a haptic feedback, and apply the steering torque when active in order to stay in ego lane.
EPS ECU - Lane Departure Warning Safety Functionality	Ensure that the lane departure oscillating torque amplitude is below“Max_Torque_Amplitude” and ensure that the lane departure oscillating torque frequency is below “Max_Torque_Frequency”
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure that the lane keeping assistance torque is applied for only Max_Duration.
EPS ECU - Final Torque	Synthesis difference input and calculate final torque output.

Motor	Generate corresponding steering torque according to the instruction from Electronic Power Steering ECU.

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 software component	the lane departure warning talk request amplitude shall be set to zero
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 software component	the lane departure warning talk request amplitude shall be set to zero
Technical Safety Requirement	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and	C	50 ms	LDW safety software component	the lane departure warning talk request

03	the 'LDW_Torque_Request' shall be set to zero.				amplitude shall be set to zero
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	N/A
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	the lane departure warning talk 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:

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 software component	the lane departure warning talk request amplitude shall be set to zero

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 software component	the lane departure warning talk request amplitude 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	50 ms	LDW safety software component	the lane departure warning talk request amplitude shall be set to zero
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	N/A
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	the lane departure warning talk request amplitude shall be set to zero

Lane Keeping Assistance (LKA) Requirements:

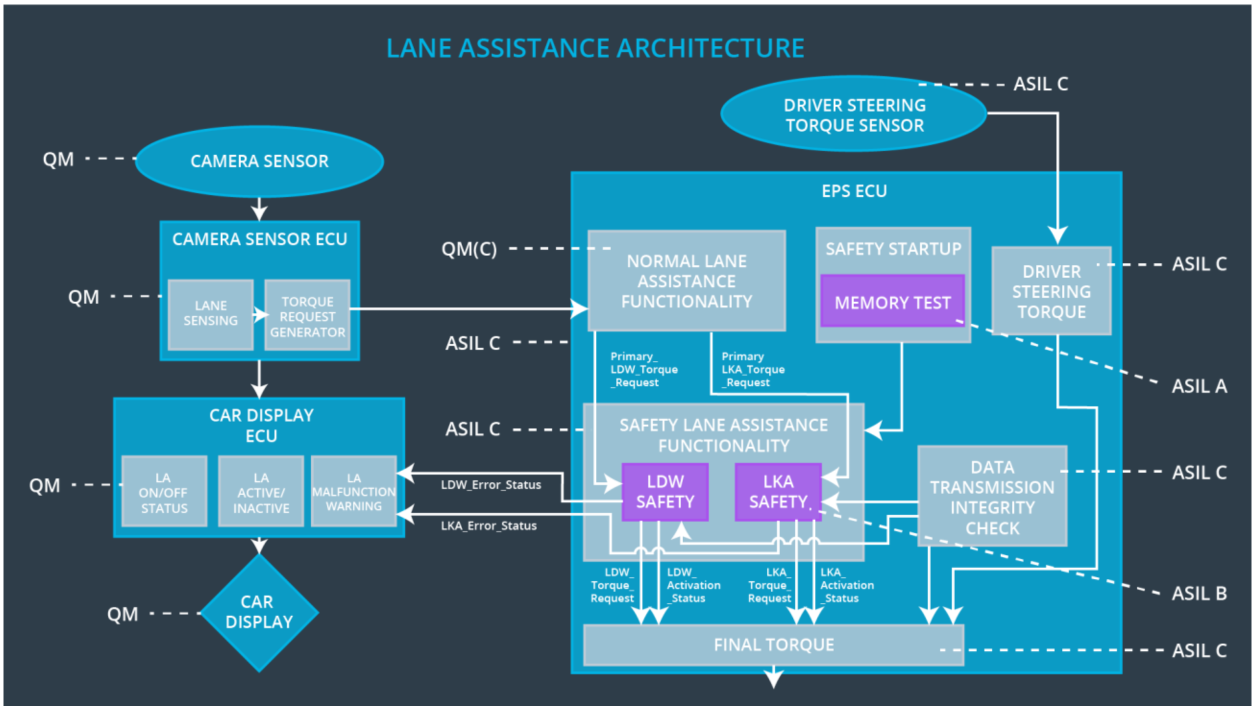
Functional Safety Requirement 02-1 with its associated system elements
(derived in the functional safety concept)

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:

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 torque of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for only 'Max_Duration '.	B	500 ms	LKA safety software component	Set lane keeping assistance torque 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 software component	Set lane keeping assistance torque 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 software component	t Set lane keeping assistance torque 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	N/A
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	Set lane keeping assistance torque 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	Turn off LDW function.	Functional Safety Requirement 01-01 / Functional Safety Requirement 01-02	Yes	Blink light on car display
WDC-02	Turn off LKA function.	Functional Safety Requirement 02-01	Yes	Blink light on car display