Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
6/4/2018	1.0	Tariq Rafique	Final Version

Table of Contents

Purpose of the Technical Safety Concept

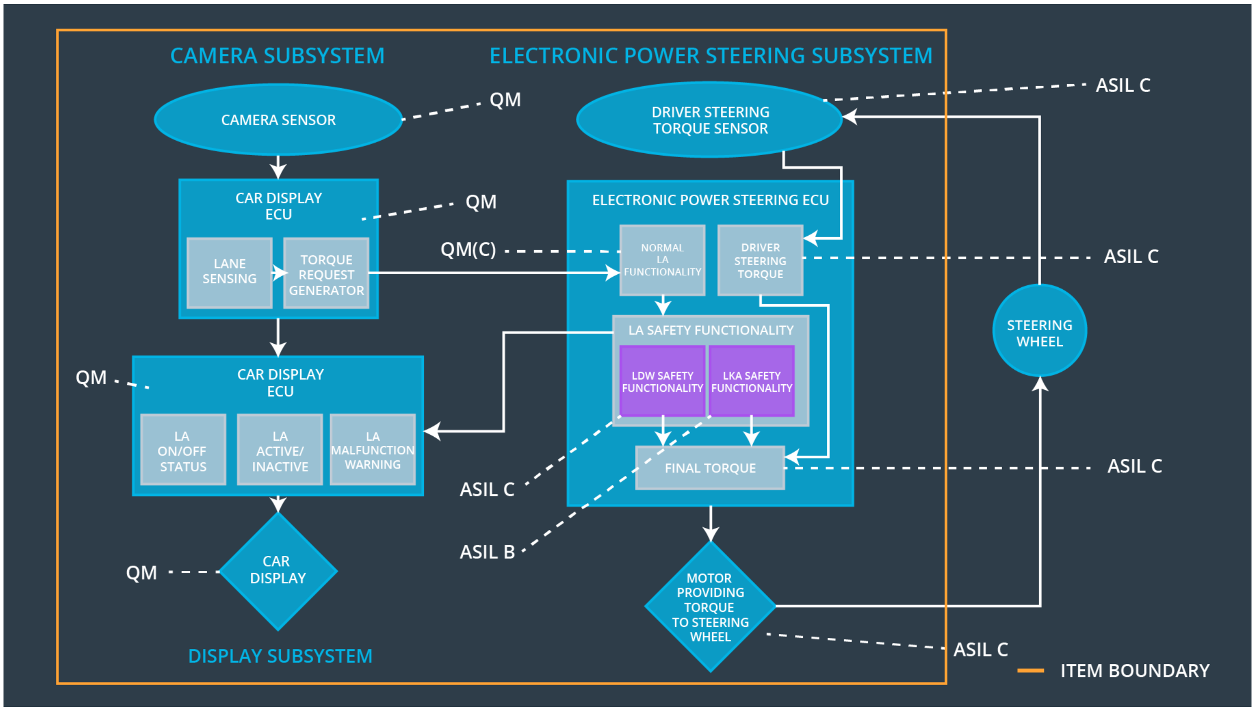
The technical safety concept defines how the subsystem interact at the message level and describes how the ECUs communicate with each other. The technical safety concept is more detailed than a functional safety concept because it looks at the details of the various subsystems.
It involves turning functional safety requirements into technical safety requirement and 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 Lane Keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Reduce torque amplitude to 0
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	Reduce vibration 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	Lane Keeping Assistance torque reduced to 0

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	The camera sensor reads in images from the front of the car and forwards them to the Camera ECU Lane Sensing
Camera Sensor ECU - Lane Sensing	Detects where the lane is in camera images and where the car is located within the lane
Camera Sensor ECU - Torque request generator	Creates a correct torque request based on where the vehicle is in the lane and where it needs to be
Car Display	Screen to show warning and information messages
Car Display ECU - Lane Assistance On/Off Status	Controls display of lane assistance status on the car display
Car Display ECU - Lane Assistant Active/Inactive	Controls display of lane assistance active/inactive status on the car display
Car Display ECU - Lane Assistance malfunction warning	Controls display of lane assistance malfunction warnings on the car display

Driver Steering Torque Sensor	Sensor that measures the amount and direction of torque applied by the driver to the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads from sensor that measures the amount and direction of torque applied by the driver to the steering wheel
EPS ECU - Normal Lane Assistance Functionality	Implements LDW and LKA functionality. Received torque requests from the Camera ECU Torque request generator and generates sterring torque
EPS ECU - Lane Departure Warning Safety Functionality	Safety module to ensure that LDW torque doesn't exceed maximum amplitude and frequency limits.
EPS ECU - Lane Keeping Assistant Safety Functionality	Safety module to ensure that the LKA functionality doesn't stay activated longer than a maximum duration
EPS ECU - Final Torque	Reads in data from driver steering torque sensor and the LDW and LKA safety module to generate the final torque for the motor
Motor	Applies torque 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	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	LDW_Torque_Request=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	50ms	LDW Safety	LDW_Torque_Request=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	50ms	LDW Safety	LDW_Torque_Request=0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	LDW_Torque_Request=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=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	The lane keeping item shall	X		

Requirement 01-02	ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency			

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	50ms	LDW Safety	LDW_Torque_Request=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	50ms	LDW Safety	LDW_Torque_Request=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	50ms	LDW Safety	LDW_Torque_Request=0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50ms	Data Transmission Integrity Check	LDW_Torque_Request=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=0

Lane Keeping Assistance (LKA) Requirements:

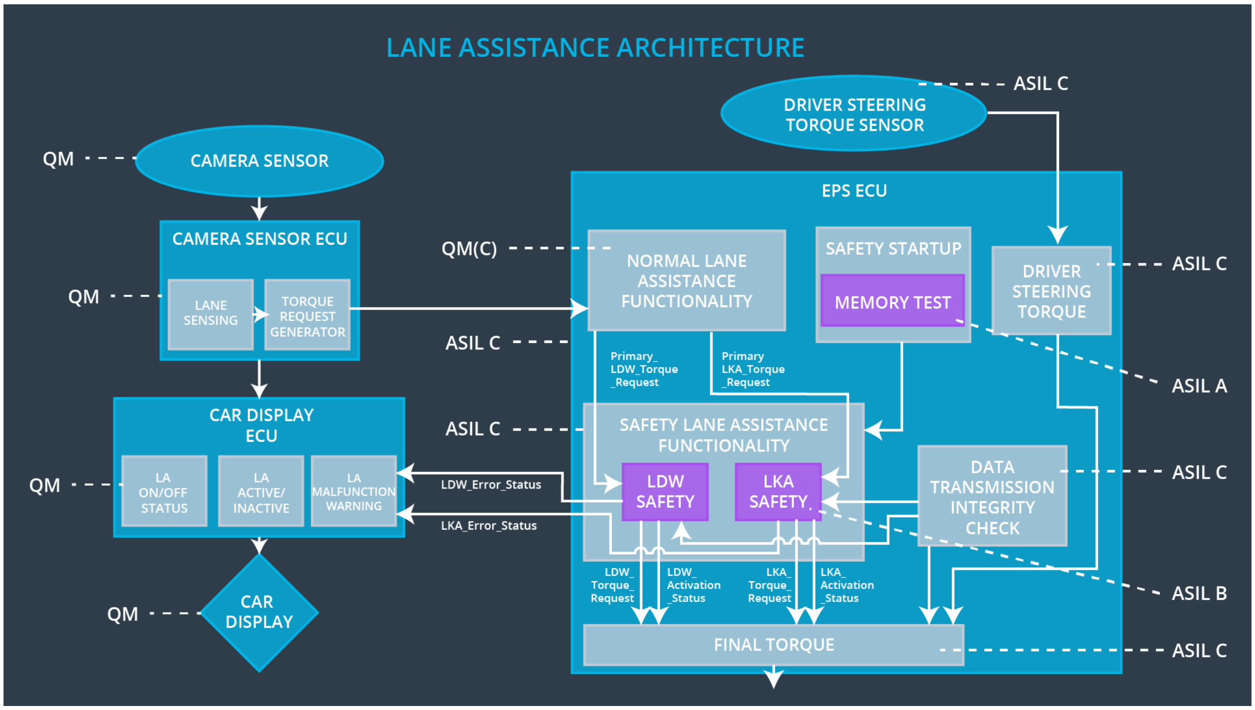
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

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 LKA Torque is only applied for Max_Duration time	B	500ms	LKA Safety	LKA_Torque_Request=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	500ms	LKA Safety	LKA_Torque_Request=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	500ms	LKA Safety	LKA_Torque_Request=0
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity Check	LKA_Torque_Request=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=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 Lane Departure Warning function	Malfunction_01 Malfunction_02	Yes	Warning light on dashboard
WDC-02	Turn off Lane Keeping Assistance function	Malfunction_03	Yes	Warning light on dashboard