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
27/11/2018	1.0	Archit Rastogi	First pass

Table of Contents

Purpose of the Technical Safety Concept

Technical safety concept involves:

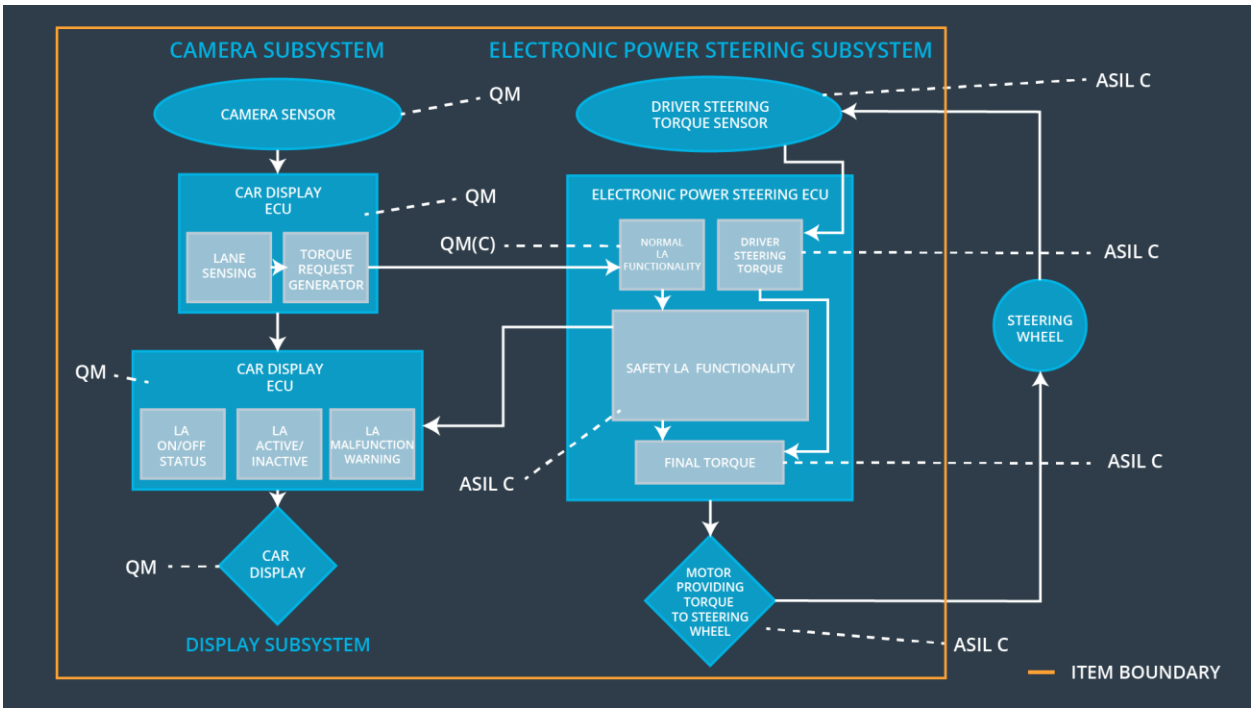
- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Vibration Torque Amplitude below Max_Torque_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	Vibration Torque frequency below Max_Torque_Frequency
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 is zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures Image and provides the data to the Camera ECU
Camera Sensor ECU - Lane Sensing	Detects Lane line from the images
Camera Sensor ECU - Torque request generator	Generates torque request based on the lane lines and position of vehicle to be sent to EPS ECU
Car Display	Show warning to the driver
Car Display ECU - Lane Assistance On/Off Status	Indicates if the LA functionality is off or on
Car Display ECU - Lane Assistant Active/Inactive	Indicates if the LA functionality is active/ inactive based on lane detection
Car Display ECU - Lane Assistance malfunction warning	Indicates any malfunction in the LA system

Driver Steering Torque Sensor	Measures the steering torque applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Process input from Driver Steering Torque Sensor
EPS ECU - Normal Lane Assistance Functionality	Receives Camera Sensor Torque request and pass it to safety lane assistance functionality module
EPS ECU - Lane Departure Warning Safety Functionality	Ensures if the LDW is working properly and the functional safety requirements are met
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensures if the LKA is working properly and the functional safety requirements are met
EPS ECU - Final Torque	Combines the torque request from LDW, LKA and also the driver steering torque and send it to the motor
Motor	Applies the final torque received from Electronic Power Steering ECU to 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 Amplitude to 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	50ms	LDW Safety	LDW_Torque_Request Amplitude to 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	LDW_Torque_Request Amplitude to 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	50ms	Data Transmission and Integrity	LDW_Torque_Request Amplitude to 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	LDW_Torque_Request Amplitude to 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	50ms	LDW Safety	LDW_Torque_Request Frequency to 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	50ms	LDW Safety	LDW_Torque_Request Frequency to 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	LDW_Torque_Request Frequency to 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	50ms	Data Transmission and Integrity	LDW_Torque_Request Frequency to 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	LDW_Torque_Request Frequency to 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)

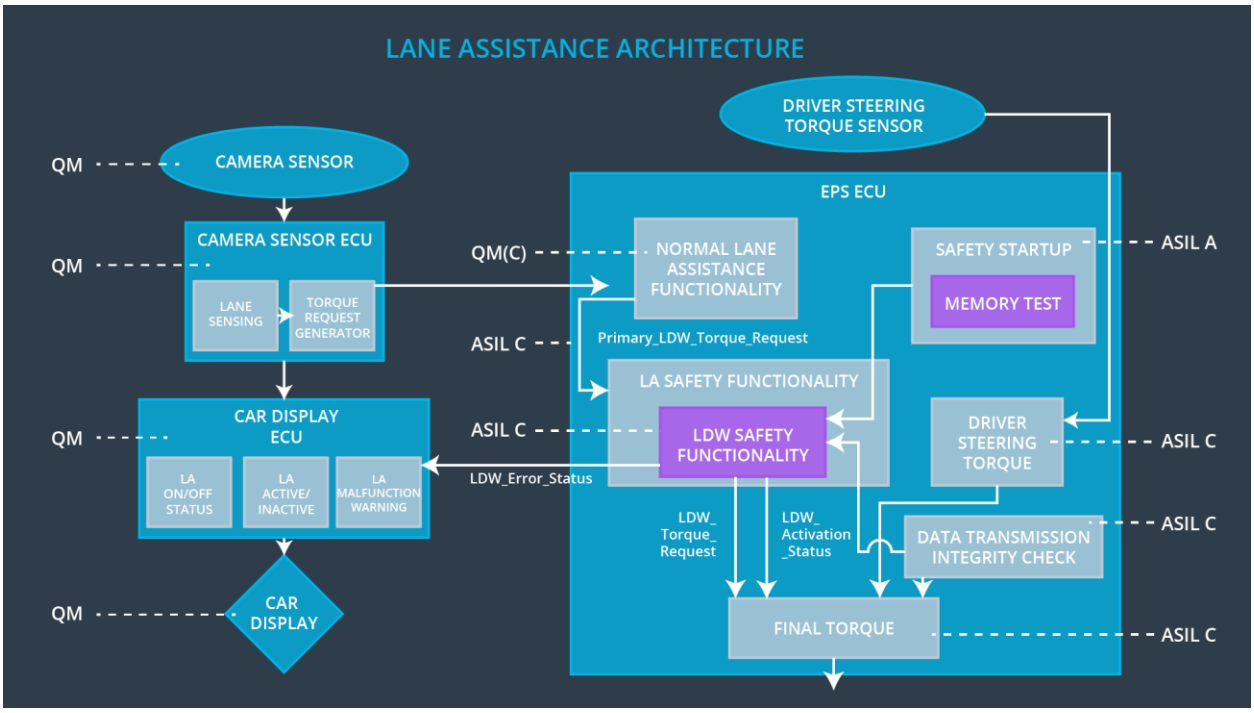
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 'LDW_Torque_Request' is sent to the 'Final electronic power steering Torque' component only for 'Max_Duration'	B	500ms	LKA Safety	LKA_Torque_Request to be set to zero
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 to 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	LKA_Torque_Request to be set to zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	Data Transmission and Integrity	LKA_Torque_Request to 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	LKA_Torque_Request to be set to zero

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	System off	Malfunction 01, 02	Yes	Warning on Car Display
WDC-02	System off	Malfunction 03	Yes	Warning on Car Display