Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version 1.0

Document history

Date	Version	Editor	Description
11/24/17	1.0	Chris Ferone	First draft of document.

Table of Contents

Purpose of the Technical Safety Concept

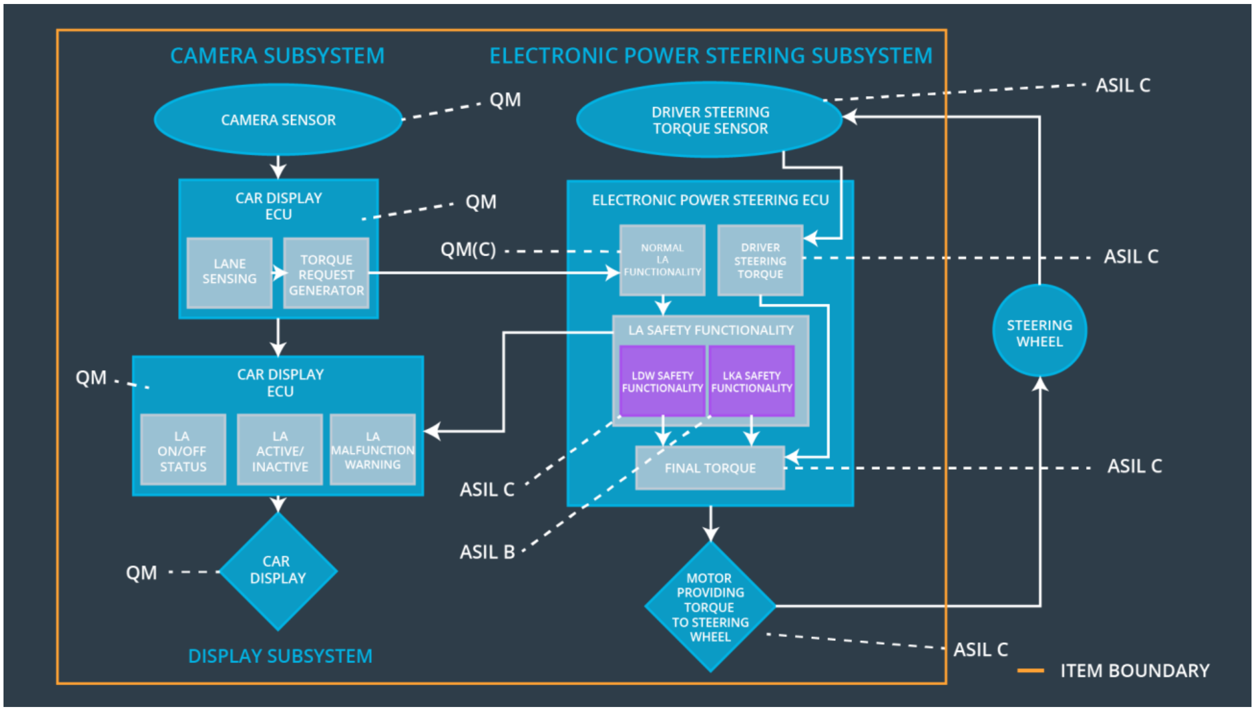
The purpose of the technical safety concept is look in greater detail at functional safety requirements. These requirements oftentimes define signal flow and look at the system elements and components.

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_Available.	C	50ms	turn off the functionality
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	turn off the functionality
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	turn off the functionality

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Captures raw image of lane
Camera Sensor ECU - Lane Sensing	Detect lane lines within image
Camera Sensor ECU - Torque request generator	Determine torque needed to move vehicle back into lane
Car Display	Notifies driver if LDW and LKA are enabled and when they become active
Car Display ECU - Lane Assistance On/Off Status	Notify driver LKA is on/off
Car Display ECU - Lane Assistant Active/Inactive	Notify driver LKA is active/inactive
Car Display ECU - Lane Assistance	Notify driver LKA system has malfunctioned

malfunction warning	
Driver Steering Torque Sensor	Measures torque applied to steering wheel by driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Adjust final torque request based on driver steering torque input
EPS ECU - Normal Lane Assistance Functionality	Passes torque requests from Camera Sensor ECU to Safety Functionality module
EPS ECU - Lane Departure Warning Safety Functionality	Passes LDW torque request to final torque module if memory and data integrity checks pass
EPS ECU - Lane Keeping Assistant Safety Functionality	Passes LKA torque request to final torque module if memory and data integrity checks pass
EPS ECU - Final Torque	Final Motor Torque request, after limits are applied, commanded by EPS
Motor	Applies torque to steering column

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 software component	The LDW torque request amplitude 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	N/A
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and	C	50ms	LDW safety software component	The LDW torque request

ent 03	the ‘LDW_Torque_Request’ shall be set to zero.				amplitude shall be set to zero
Technical Safety Requirement 04	As soon at 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 software component	The LDW torque request amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Length of vehicle ignition cycle	Safety Startup – Memory Test	The 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:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety	The LDW safety component shall ensure that the frequency of the	C	50ms	LDW safety software	The LDW

Requirement 01	‘LDW_Torque_Request’ sent to the ‘Final electronic power steering Torque’ component is below ‘Max_Torque_Frequency’			component	torque request frequency 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	N/A
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 software component	The LDW torque request frequency shall be set to zero
Technical Safety Requirement 04	As soon at 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 software component	The LDW torque request frequency shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Length of vehicle ignition cycle	Safety Startup – Memory Test	The LDW torque request frequency 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		

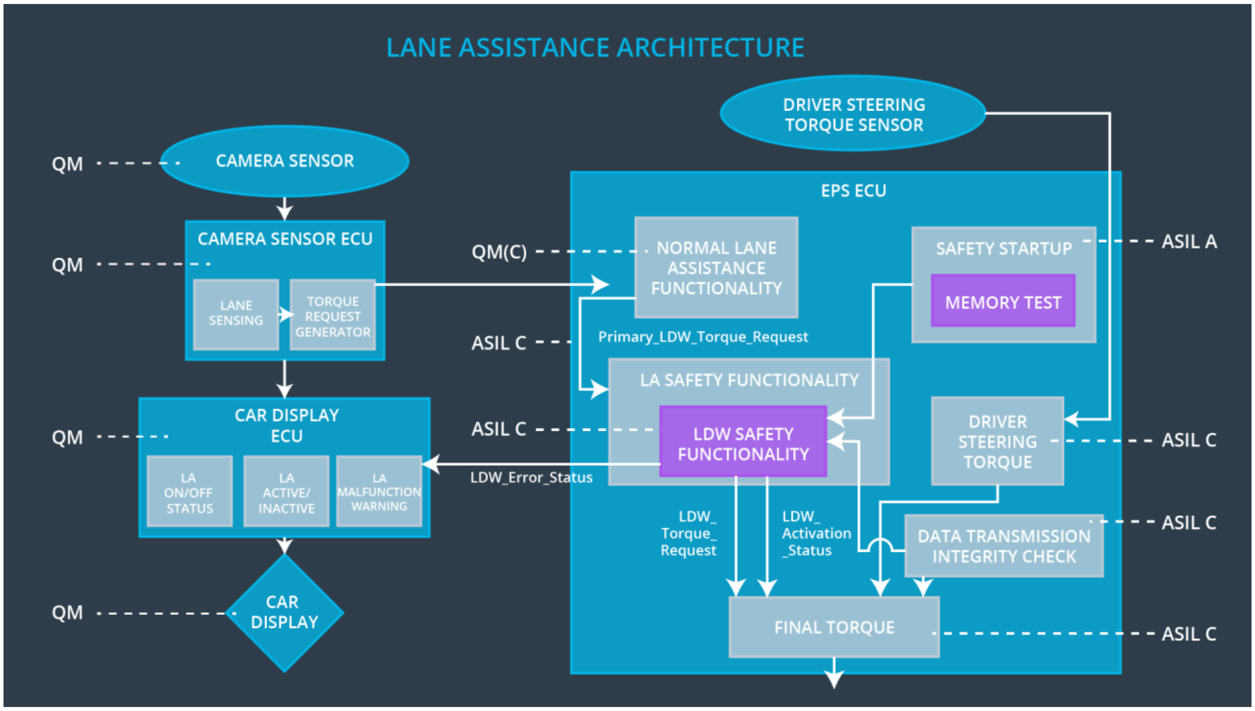
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that that 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is applied for only Max_Duration	B	500ms	LKA safety software component	The LKA torque request 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	N/A
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 software component	The LKA torque request shall be set to zero
Technical Safety Requireme	As soon at the LKA function deactivates the LKA feature, the	B	500ms	LKA safety software component	The LKA torque

nt 04	‘LKA Safety’ software block shall send a signal to the car display ECU to turn on a warning light.				request shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Length of vehicle ignition cycle	Safety Startup – Memory Test	The LKA torque request 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 the functionality	Malfunction_01, Malfunction_02	Yes	warning light on the dashboard
WDC-02	turn off the functionality	Malfunction_03	Yes	warning light on the dashboard