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
19/08/2018	1.0	Jumana MP	First Attempt

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to refine the functional safety requirements established in the functional safety concept into technical safety requirements. This step is taken before any software and hardware development to ensure that all components when

designed meets their respective safety requirements. As a part of product development, technical safety concept involves:

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

As a subsequent step, technical safety requirements will be considered within the software and hardware implementation.

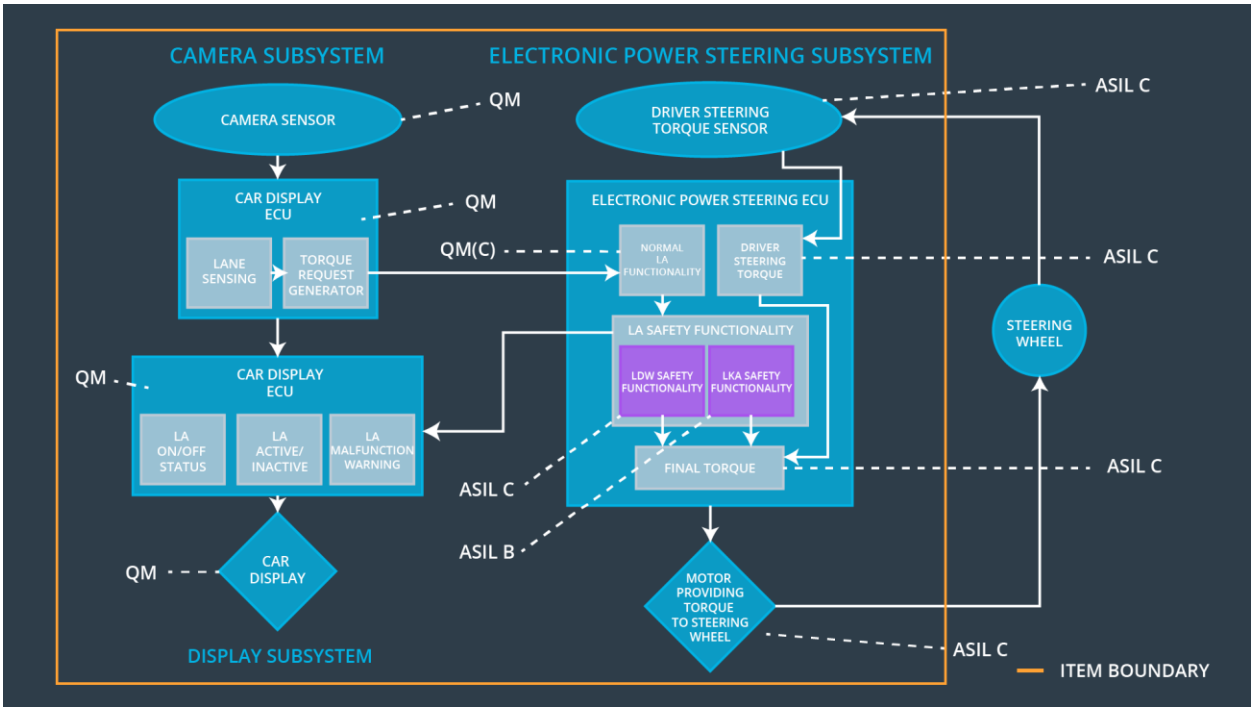
Inputs to the Technical Safety Concept

Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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 warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Deactivate the function
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Deactivate the function
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the it stops applying the steering torque to direct car towards the center of the lane after a certain amount of time.	B	500ms	Deactivate the function
Functional Safety Requirement 02-02	The lane assistance item shall ensure that it stops working in weather conditions where camera sensor fails.	A	10ms	Deactivate the function
Functional Safety Requirement 02-03	The lane assistance item shall ensure that it takes wind force into account while computing required torque for car steering.	C	10ms	Alert the driver with alarm and verify driver is in control.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	Captures lame images and sends to the Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	Detects lane line positions from the camera images.
Camera Sensor ECU - Torque request generator	Generates torque requests to the EPS ECU after evaluating the lane position data from the camera sensor ECU.

Car Display	Displays warning and status messages from the item to the driver.
Car Display ECU - Lane Assistance On/Off Status	Indicate if the LA functionality is powered on.
Car Display ECU - Lane Assistant Active/Inactive	Indicate if the LA functionality is active at the moment.
Car Display ECU - Lane Assistance malfunction warning	Informs if there is a malfunction detected in the LA functionality.
Driver Steering Torque Sensor	Senses the intensity of the torque being provided by the driver to the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Processes the input torque being provided by the driver to the steering wheel.
EPS ECU - Normal Lane Assistance Functionality	Processes the input torque request from the car sensor ECU torque request generator and pass the data to the LDW Safe software block.
EPS ECU - Lane Departure Warning Safety Functionality	Checks for malfunctions in the LDW functionality.
EPS ECU - Lane Keeping Assistant Safety Functionality	Checks for malfunctions in the LKA functionality.
EPS ECU - Final Torque	Generates final torque from the input from both the Lane Assistance Safety functionality and the Electronic Power Steering (EPS) ECU - Driver Steering Torque
Motor	Applies the final torque obtained from the EPS ECU - Final Torque component 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

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 block	LDW torque output is 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 Software block	LDW torque output is 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 Software block	LDW torque output is 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 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	LDW torque output is 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 Software block	LDW torque output is 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 Software block	LDW torque output is 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 Software block	LDW torque output is 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 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	LDW torque output is set to zero

Lane Keeping Assistance (LKA) Requirements:

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

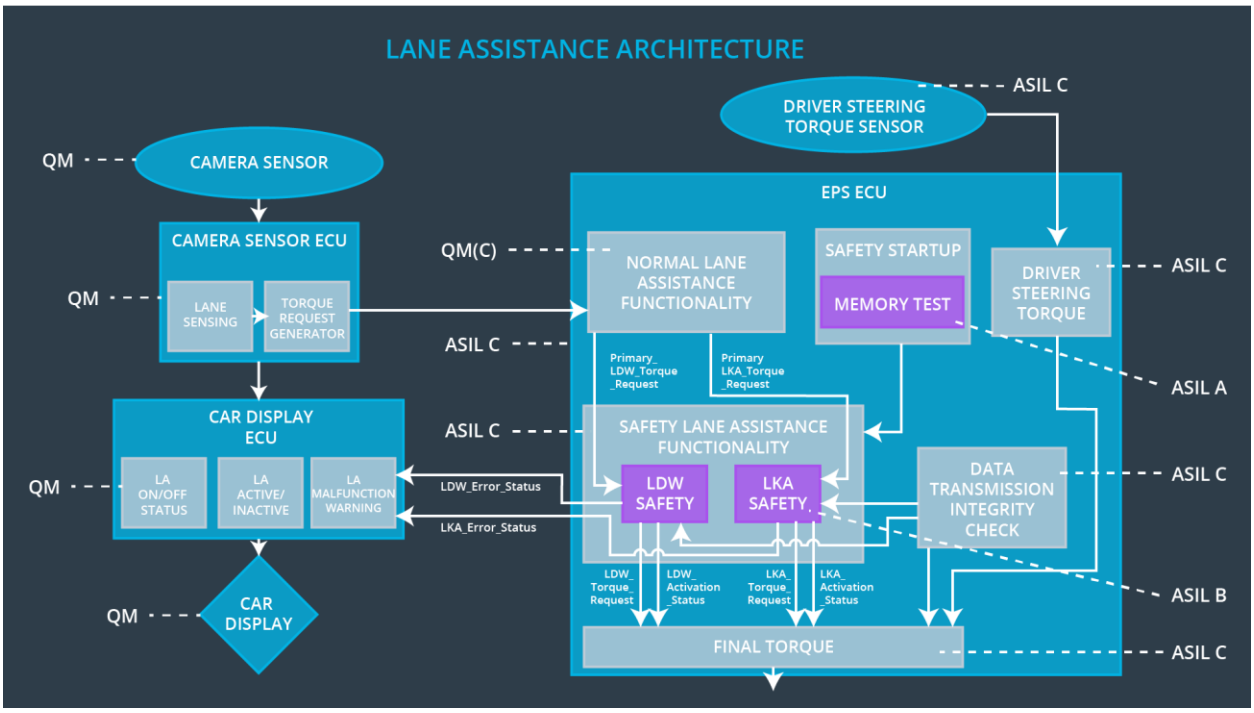
ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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

ID	Technical Safety Requirement	AS	Fault Tolerant	Allocation to Architecture	Safe State

		IL	Time Interval		
Technical Safety Requirement 01	The LKA safety component shall ensure that the frequency of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is only for 'Max_Duration.	B	500ms	LKA Safety Software block	LKA Activation status is zero
Technical Safety Requirement 02	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 block	LKA Activation status is zero
Technical Safety Requirement 03	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 Software block	LKA Activation status is zero
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500ms	LKA Safety Software block	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.	B	500ms	LKA Safety Software block	LKA Activation status is zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU. Refer tables above for more details.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the LDW function	Malfunction_01	Yes	Warning on Car display dashboard
WDC-02	Turn off the LKA function	Malfunction_02	Yes	Warning on Car display dashboard
WDC-03	Turn off the LDW function	Malfunction_03	Yes	Warning on Car display dashboard
WDC-04	Turn off the LDW function	Malfunction_04	Yes	Warning on Car display dashboard

WDC-05	Alarm the driver to be in control.	Malfunction_05	Yes	Warning on Car display dashboard