Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
11/21/2018	1.0	Claris Li	Initial draft
11/22/2018	1.1	Claris Li	Update FTTI in Technical Safety Requirement 01-02-05 and ASIL in Technical Safety Requirement 02-01

Table of Contents

Warning and Degradation Concept

Purpose of the Technical Safety Concept

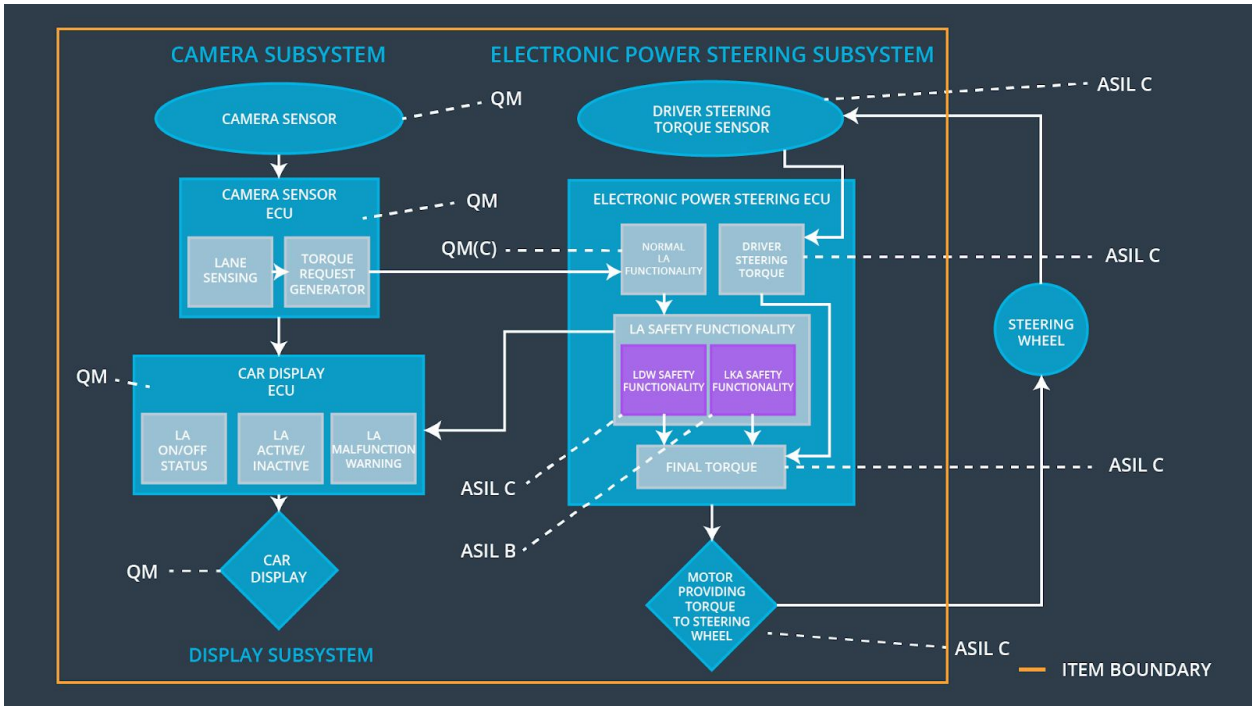
The purpose is to look at the safety requirements in a more concrete way at the level of sensors, control unit, and actuator, and then refine the system architecture accordingly.

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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	LDW torque output is set to zero
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	LDW torque output is set to zero
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	500 ms	LKA torque output is set to zero

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Take pictures and send them to the camera sensor ECU
Camera Sensor ECU - Lane Sensing	Analyze the input images to detect lane departures
Camera Sensor ECU - Torque request generator	Calculate and determine how much the steering wheel should turn
Car Display	Provide visual feedback to the driver to display warnings
Car Display ECU - Lane Assistance	Control the car display to the On/Off status of

On/Off Status	Lane Assistance as requested by the camera sensor ECU
Car Display ECU - Lane Assistant Active/Inactive	Control the car display to the Active/Inactive status of Lane Assistance
Car Display ECU - Lane Assistance malfunction warning	Control the car display warning of Lane Assistance malfunction
Driver Steering Torque Sensor	Detect the amount of torque been applied by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Receive the driver's torque from sensor and send it to FINAL TORQUE
EPS ECU - Normal Lane Assistance Functionality	Receive the torque request from Camera Sensor ECU and send Primary_LDW_Torque_Request to LA Safety functionality
EPS ECU - Lane Departure Warning Safety Functionality	Ensure the torque amplitude sent to FINAL TORQUE is below Max_Torque_Amplitude and torque frequency is below Max_Torque_frequency.
EPS ECU - Lane Keeping Assistant Safety Functionality	Ensure torque is applied under Max_Duration.
EPS ECU - Final Torque	Combine the torque requests from Lane Departure Warning, Lane Keeping, and Driver Steering Torque and send it to the motor.
Motor	Apply the requested torque to the steering wheels.

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	LDW torque output is set to zero
Technical Safety Requirem	As soon as a failure is detected by the LDW function, it shall deactivate	C	50 ms	LDW Safety	LDW torque output is set to zero

ent 02	the LDW feature and the 'LDW_Torque_Request' shall be set to zero.				
Technical Safety Requirement 03	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	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	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	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	50 ms	LDW Safety	LDW torque output is set to zero
Technical Safety Requirement 02	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	LDW torque output is set to zero
Technical Safety Requirement 03	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	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	50 ms	Data Transmission Integrity Check	N/A
Technical Safety Requirement	Memory test shall be conducted at start up of the EPS ECU to check for any	A	Ignition cycle	Memory Test	LDW torque output

05	faults in memory.				is set to zero

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01-01-01	Validate Max_Torque_Amplitude is the chosen value from functional safety concept.	Verify LDW is off when Max_Torque_Amplitude is not set to the chosen value.
Technical Safety Requirement 01-01-02	Validate the LDW Safety sets LDW_Torque_Request to zero when LDW deactivates.	Verify LDW is off when LDW_Torque_Reqeust is not set to zero when LDW deactivates.
Technical Safety Requirement 01-01-03	Validate the LDW Safety sends a malfunction LDW_Error_Status to Car Display ECU when LDW deactivates	Verify the Car Display displays the LDW malfunction warning.
Technical Safety Requirement 01-01-04	Validate 'LDW_Torque_Request' is sent and received correctly with CRC and Alive Counter.	Verify LDW is off when LDW_Torque_Request is not sent and received correctly.
Technical Safety Requirement 01-01-05	Validate Memory Test catches memory faults.	Verify LDW is off when Memory Test doesn’t work properly.
Technical Safety Requirement 01-02-01	Validate Max_Torque_Frequency is the chosen value from functional safety concept.	Verify LDW is off when Max_Torque_Frequency is not set to the chosen value.

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 Lane Keeping Assistance Safety Component shall ensure the duration of torque applied is less than Max_Duration.	B	500 ms	LKA Safety	LKA sets torque to 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	500 ms	LKA Safety	LKA sets torque to zero.
Technical Safety Requirem	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block	B	500 ms	LKA Safety	LKA sets torque to zero.

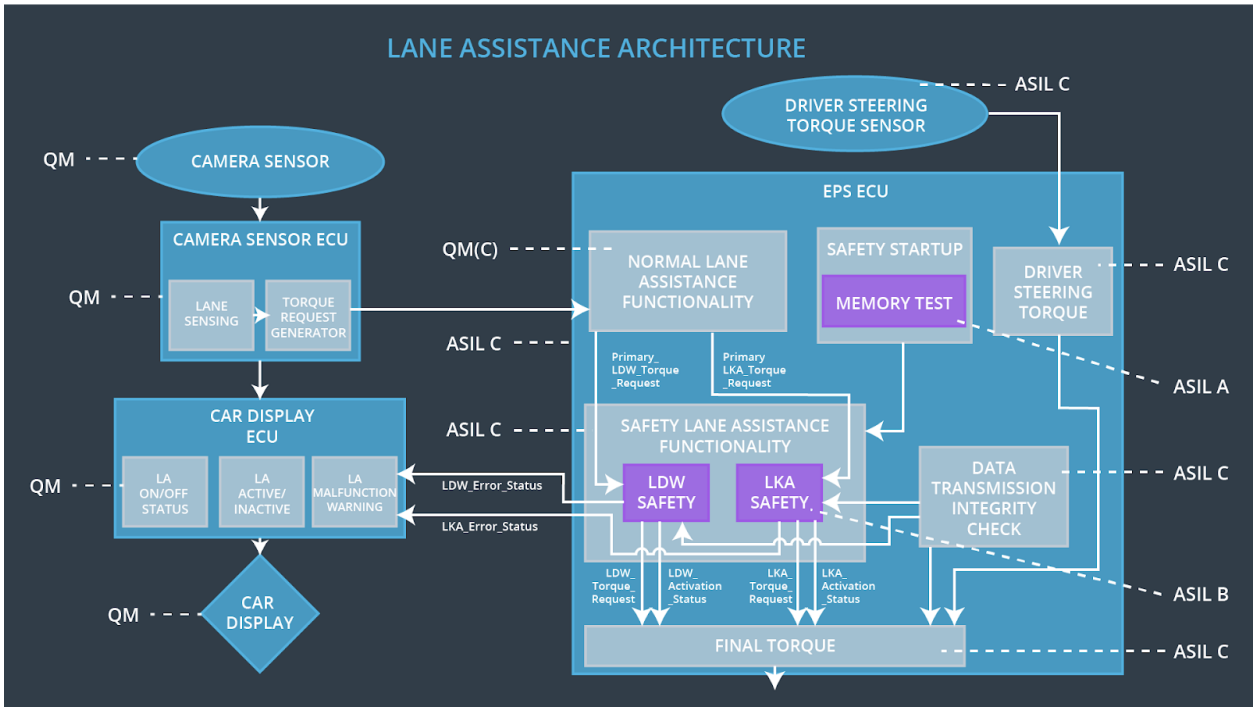
ent 03	shall send a signal to the car display ECU to turn on a warning light.				
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	N/A
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	LKA sets torque to zero.

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 02-02-01	Validate the Max_Duration chosen is the chosen value the functional safety concept.	Verify LKA is off when Max_Duration is not set to the chosen value.
Technical Safety Requirement 02-01-02	Validate the LKA Safety sets LKA_Torque_Request to zero when LKA deactivates.	Verify LKA is off when LKA_Torque_Reqeust is not set to zero when LKA deactivates.
Technical Safety Requirement 02-01-03	Validate the LKA Safety sends a malfunction LKA_Error_Status to Car Display ECU when LKA deactivates	Verify the Car Display displays the LKA malfunction warning.
Technical	Validate 'LKA_Torque_Request' is	Verify LKA is off when

Safety Requirement 02-01-04	sent and received correctly with CRC and Alive Counter.	LKA_Torque_Request is not sent and received correctly.
Technical Safety Requirement 02-01-05	Validate Memory Test catches memory faults.	Verify LKA is off when Memory Test doesn't work properly.

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 the LDW off	Malfunction_01, Malfunction_02, Malfunction_05	Yes	Show the LDW Malfunction Warning on Car Display
WDC-02	Turn the LKA off	Malfunction_03, Malfunction_04	Yes	Show the LKA Malfunction Warning on Car Display