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
14/05/2018	1.0	Sundeep Pundamale Selvaraj	First Draft

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept

- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept

Functional overview of architecture elements

Technical Safety Concept
Technical Safety Requirements
Refinement of the System Architecture
Allocation of Technical Safety Requirements to Architecture Elements
Warning and Degradation Concept

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]

The Technical Safety Concept defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

Functional Safety Requirements

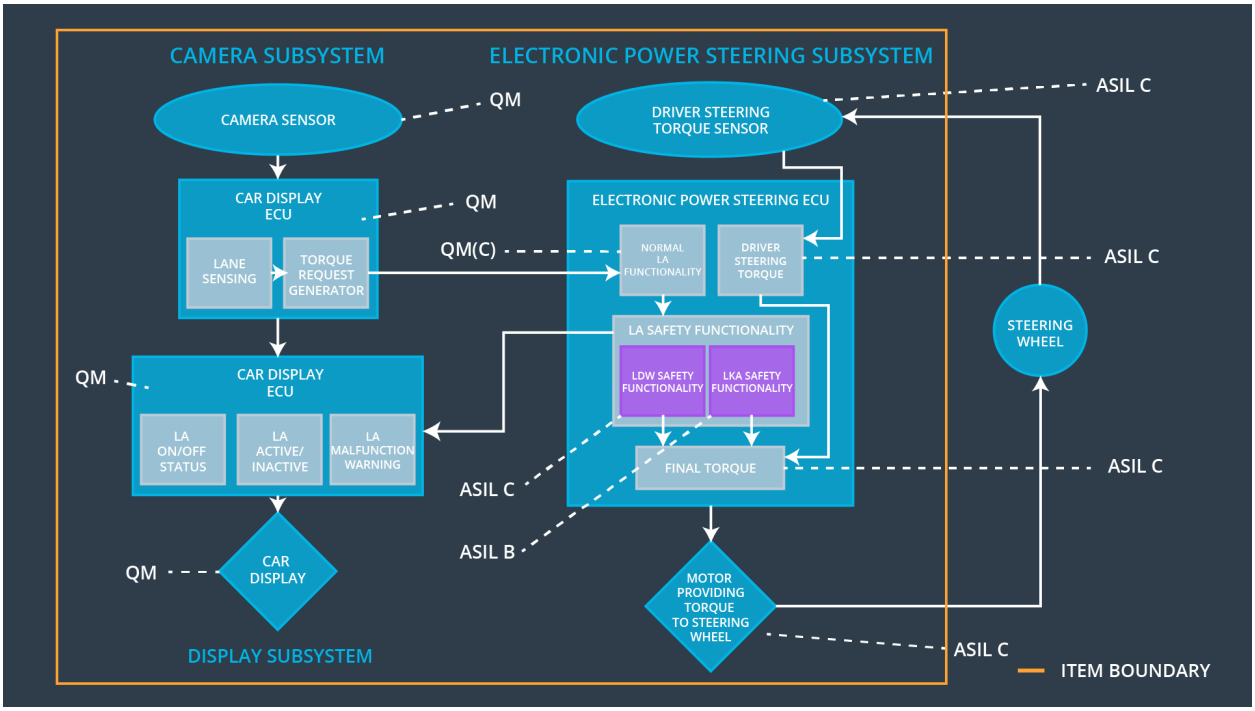
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The Lane Departure Warning function shall ensure that the lane departure torque amplitude is always below the Max_Torque_Amplitude	C	50 MS	The torque amplitude is always below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The Lane Departure Warning functional shall ensure that the lane departure torque amplitude is always below the Max_Torque_Frequency	C	50 MS	The torque frequency is always below the Max_Torque_Frequency
Functional Safety Requirement 02-01	The Lane Keeping Assistance Warning shall ensure that the torque is applied on the steering for a Max_Duration only	C	500 MS	The Lane Keeping Assistance torque value is

				zero

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the 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	The camera sensor reads the road images and provides the data to Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	The Camera Sensor ECU – Lane Sensing detects the lane line positions from the camera images

Camera Sensor ECU - Torque request generator	The Camera Sensor ECU – Torque request generator calculates the torque and generates a request to the Electronic Power Steering ECU
Car Display	The car display provides visual notification to warn the driver about the Lane departure status
Car Display ECU - Lane Assistance On/Off Status	The car Display ECU - Lane Assistance On/Off Status indicates if the Lane Assistance is On or Off
Car Display ECU - Lane Assistant Active/Inactive	The car Display ECU - Lane Assistant Active/Inactive indicates if the Lane Assistant function is in Active or Inactive state
Car Display ECU - Lane Assistance malfunction warning	The car Display ECU - Lane Assistance malfunction warning indicates a fault in the Lane Assistance system
Driver Steering Torque Sensor	The driver steering torque sensor measures the torque applied by the driver on the steering wheel
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The Electronic Power Steering (EPS) ECU - Driver Steering Torque receives and processes the input from the driver steering torque sensor
EPS ECU - Normal Lane Assistance Functionality	The EPS ECU - Normal Lane Assistance Functionality receives and processes the torque request received from Camera Sensor ECU
EPS ECU - Lane Departure Warning Safety Functionality	The EPS ECU - Lane Departure Warning Safety Functionality detects the malfunction of the Lane Departure Warning and limits the torque such that it does not exceed the Max_Torque_Amplitude and the Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	The EPS ECU - Lane Keeping Assistant Safety Functionality ensures that the functionality is not active for more than Max_Duration time
EPS ECU - Final Torque	The EPS ECU - Final Torque collects the request from Lane Keeping Assistance and Lane Departure Assistance warning functionalities and sends the combined torque request to the motor
Motor	The motor applies the torque to the steering wheel as notified by the Electronic power steering ECU

Technical Safety Concept

Technical Safety Requirements

[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]

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 Lane Departure Warning safety component shall ensure that the amplitude of the LDW_Torque_Request sent to the Final electronic power steering torque is below the Max_Torque_Amplitude	C	50 MS	LDW Safety	Lane departure warning torque is set to Zero
Technical	The Lane Departure Warning	C	50 MS	LDW Safety	Lane

Safety Requirement 02	shall be de-activated and the LDW_Torque_Request is set to zero when a failure is detected in the Lane Departure Warning system				departure warning torque is set to Zero
Technical Safety Requirement 03	The Lane Departure Warning shall send a signal to the car display ECU to turn on the warning signal when the Lane Departure Warning system is deactivated	C	50 MS	LDW Safety	Lane departure warning torque 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	Lane departure warning torque is set to Zero
Technical Safety Requirement 05	Memory tests shall be conducted at the startup of the EPS ECU to check for memory faults	A	Ignition Cycle	Memory Check	Lane departure warning torque is set to Zero

[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]

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 Lane departure warning component shall make sure that frequency of the LDW_Torque_Request sent to the Final electronic power steering torque is less than the Max_Torque_Frequecy	C	50 MS	LDW safety	Lane departure warning torque is set to Zero
Technical Safety Requirement 02	The Lane departure warning component shall send a message to the car display ECU to turn on the warning signal when the function is deactivated	C	50 MS	LDW safety	Lane departure warning torque is set to Zero
Technical Safety Requirement 03	The Lane departure warning component shall deactivate the LDW feature and set the LDW_Torque_Request to zero when a failure is detected	C	50 MS	LDW safety	Lane departure warning torque 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	Lane departure warning torque is set to Zero
Technical Safety Requirement 05	Memory tests shall be conducted at the startup of the EPS ECU to check for memory faults	A	Ignition Cycle	Memory Test	Lane departure warning torque is set to Zero

Lane Keeping Assistance (LKA) Requirements:

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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		

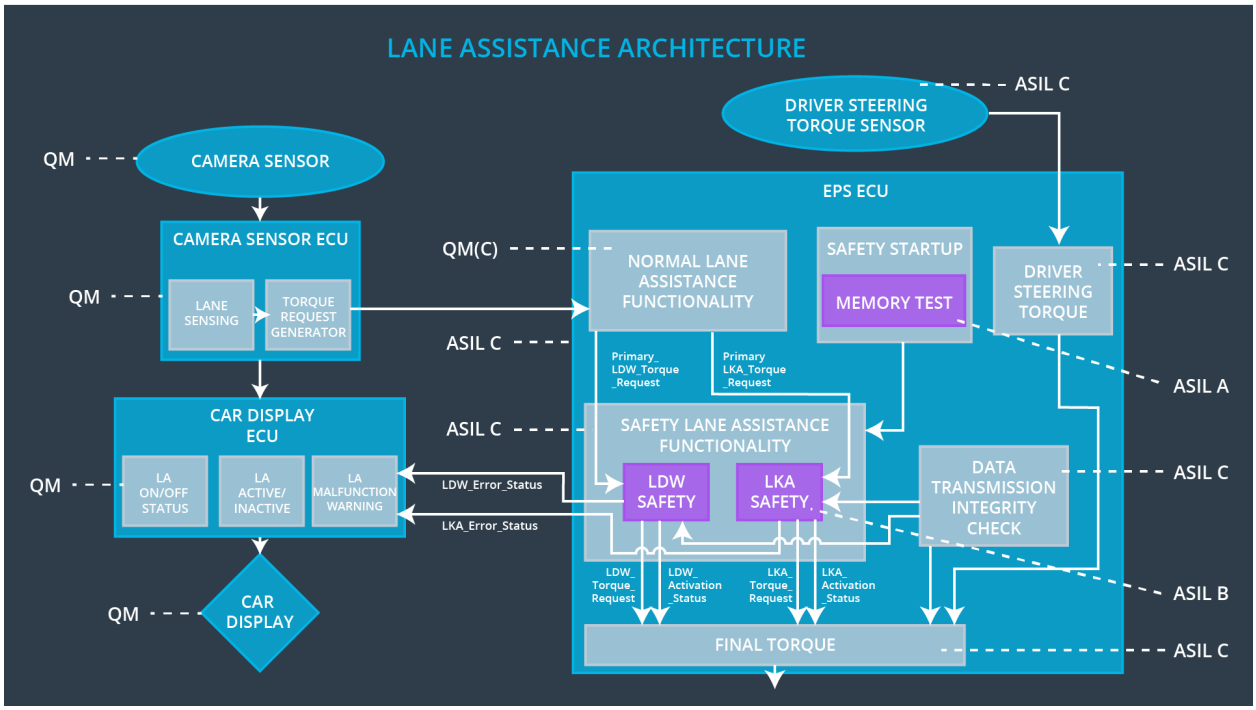
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The Lane Keeping Assistance component shall make sure that duration of toque applied during the lane keeping assistance is less than the Max_Duration	C	500 MS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 02	The Lane Keeping Assistance shall set the LKA_Torque_Request to zero when a failure is detected	C	500 MS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 03	The Lane Keeping Assistance shall send a signal to the Car Display ECU to turn on the warning light when the function is	C	500 MS	LKA Safety	Lane Keeping Assistance Torque is set to zero

	deactivated				
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured	C	500 MS	LKA Safety	Lane Keeping Assistance Torque is set to zero
Technical Safety Requirement 05	Memory tests shall be conducted at the startup of the EPS ECU to check for memory faults	A	Ignition Cycle	LKA Safety	Lane Keeping Assistance Torque is set to zero

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]



Allocation of Technical Safety Requirements to Architecture Elements

[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]

All the technical safety requirements are allocated to Electronic Power Steering ECU. The allocation are already listed in the technical requirements table in the previous sections of this document

Warning and Degradation Concept

[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.

So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.

Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the Lane Departure Warning functionality	Malfunction_01, Malfunction_04	YES	Lane departure status to be displayed as broken on the car display
WDC-02	Turn off the Lane Keeping Assistance functionality	Malfunction_02, Malfunction_03	YES	Lane keeping assistance to be displayed as broken on the car display