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
8/24/2017	V1.0	Kris Harikrishnan	Initial Document
8/25/2017	V1.1	Kris Harikrishnan	Revisions
8/26/2017	V1.2	Kris Harikrishnan	Incorporated feedback from Udacity reviewer

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]

Purpose of the Technical Safety Concept

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

Both functional and technical safety concepts involve defining new requirements and allocating them to system architecture. However, the functional safety concept is high-level and applied at the concept phase while the technical safety concept is detailed and is applied at the product development phase.

Inputs to the Technical Safety Concept

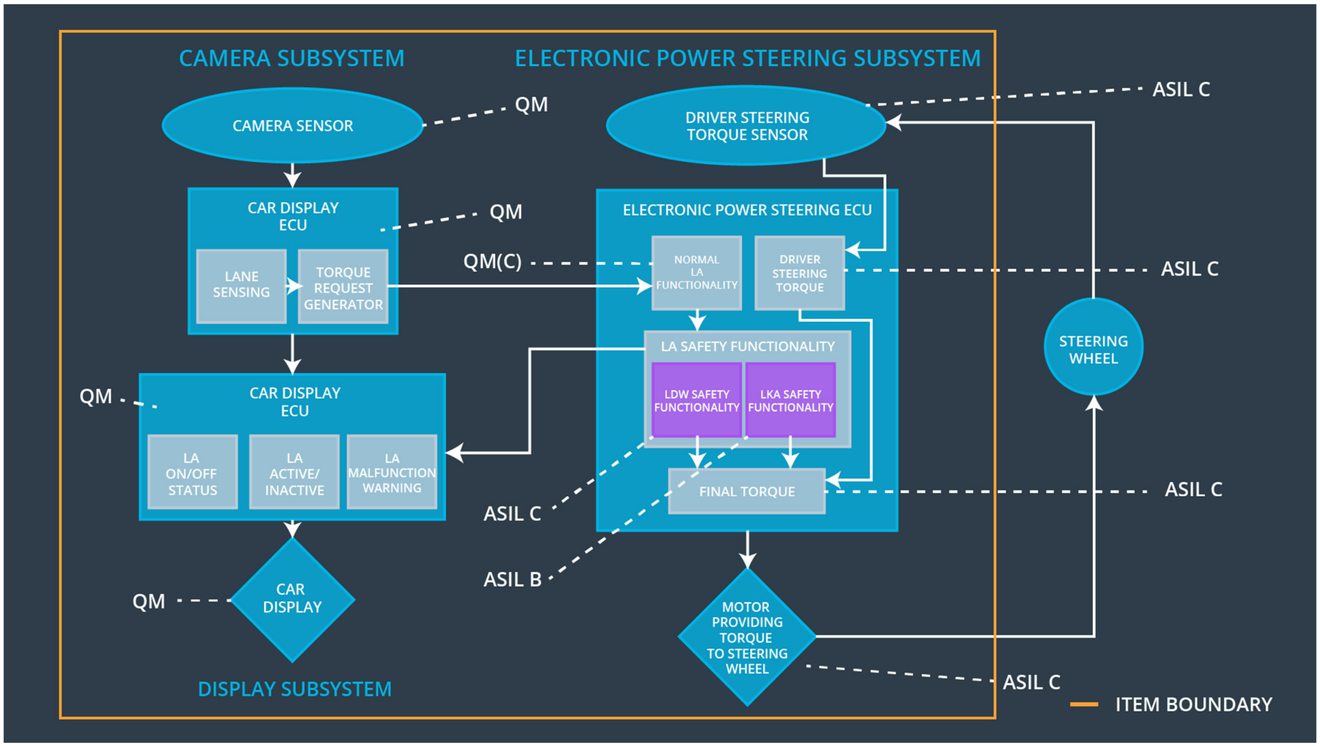
Functional Safety Requirements

[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 EPS ECU shall ensure that the lane departure warning torque amplitude is below Max_Torque_Amplitude	C	50ms	Set vibration torque amplitude to zero
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure warning torque frequency is below Max_Torque_Frequency	C	50ms	Set vibration torque frequency 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	500ms	Set lane keeping assistance torque to 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	Takes lane pictures
Camera Sensor ECU - Lane Sensing	The camera ECU system detects lane departures through deep learning and computer vision techniques
Camera Sensor ECU - Torque request generator	The camera ECU system tells the steering wheel ECU system how hard to turn
Car Display	Dashboard to display various warning information

Car Display ECU - Lane Assistance On/Off Status	Displays LDW and LKA warning On/Off status
Car Display ECU - Lane Assistant Active/Inactive	Gets a signal from LA Safety Functionality. if LDW or LKA function is deactivated, it will get “activation_status_set = 0” Otherwise, it will get ”activation_status_set = 1”
Car Display ECU - Lane Assistance malfunction warning	Gets a signal of whether or not turning on a warning light from LDW or LKA Safety Functionality software when a failure is detected
Driver Steering Torque Sensor	Measures the torque provided by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Responsible for measuring the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request
EPS ECU - Normal Lane Assistance Functionality	Receives torque request from “Camera Sensor ECU -Torque request generator” and sends Vibrational_Torque_Request to the Lane Departure Warning Safety Software Element
EPS ECU - Lane Departure Warning Safety Functionality	Receives a torque request from “EPS ECU- Normal Lane Assistance Functionality”. If the torque request is below Max_Torque_Request, the torque request is delivered to “EPS ECU -Final Torque” But if the torque request is above “Max_Torque_Request”, the “EPS ECU -Lane Departure Warning Safety Functionality” will transmit a signal “Car Display ECU -Lane Assistance malfunction warning” to turn on a warning light and also transmit torque request which is set to zero to “EPS ECU -Final Torque”
EPS ECU - Lane Keeping Assistant Safety Functionality	Gets a torque request from “EPS ECU- Normal Lane Assistance Functionality”. If the torque request is below Max_Torque_Request, the torque request is delivered to “EPS ECU -Final Torque” But if the torque request is above “Max_Torque_Request”, the “EPS ECU -Lane Keeping Warning Safety Functionality” will transmit a signal toward “Car Display ECU -Lane Assistance malfunction warning” to turn on a warning light and also transmit torque request which is set to zero to “EPS ECU -Final Torque”.
EPS ECU - Final Torque	Receives driver steering torque and torque request from “EPS ECU Lane Departure Warning Safety Functionality” and ”EPS ECU Lane Keeping

	Assistant Safety Functionality” and then transmits the torque to “Motor” only when those torque values are below maximum. If those torque values are above maximum, it will transmit zero torque request to “Motor”.
Motor	Provides torque to the steering wheel

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 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 block	LDW torque output is 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	Ignition cycle	Memory test block	LDW torque output 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	Camera	Car Display

		Power Steering ECU	**ECU**	**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 block	LDW torque output is 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	Ignition cycle	Memory test block	LDW torque output 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		

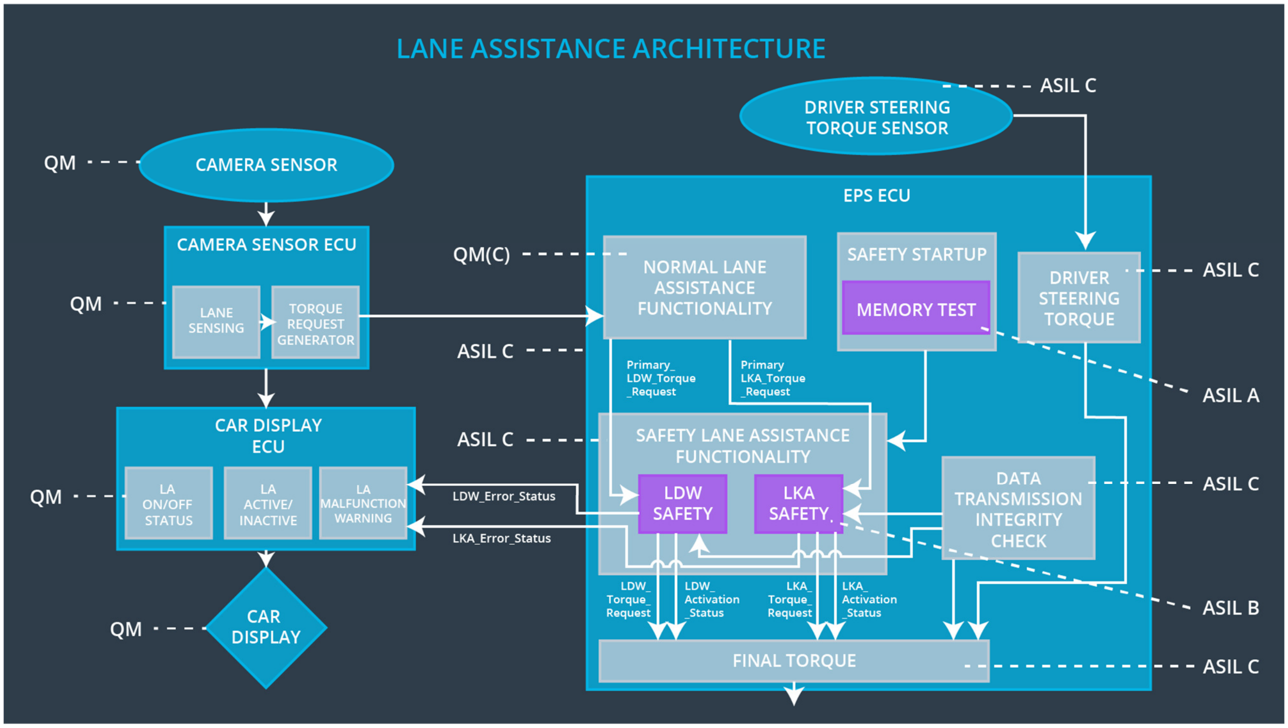
Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall ensure that the duration of the *LKA_Torque_Request* sent to the Final electronic power steering Torque component is applied for *Max_Duration*.	B	500ms	LKA Safety Software block	LKA torque output is set to zero
Technical Safety	As soon as the LKA function deactivates the LKA feature, the	B	500ms	LKA Safety Software block	LKA torque output is set

Requirement 02	LKA Safety' software block shall send a signal to the car display ECU to turn on a warning light.				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 Software block	LKA torque output is 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 integrity check block	LKA torque output is 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	Ignition cycle	Memory test block	LKA torque output 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 technical safety requirements for LDW and LKA are allocated to the electronic power steering (ECU) system.

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	Oscillating torque amplitude is above Max_Torque_Amplitude and oscillating torque frequency is above Max_Torque_Frequency	Yes	Car display
WDC-02	Turn off	Lane keeping assistance torque is applied for longer than Max_Duration	Yes	Car display