Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

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
24/05/2018	1.0	Shubhadeep	First Attempt

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?]

The purpose of a technical safety concept is to define the interaction of subsystems at message level and to describe the communication between ECUs. New requirements are being defined in this document and are assigned to the system architecture. These new requirements are more concrete and provides the details of the item's technology as specified by ISO 26262.

Inputs to the Technical Safety Concept

Functional Safety Requirements

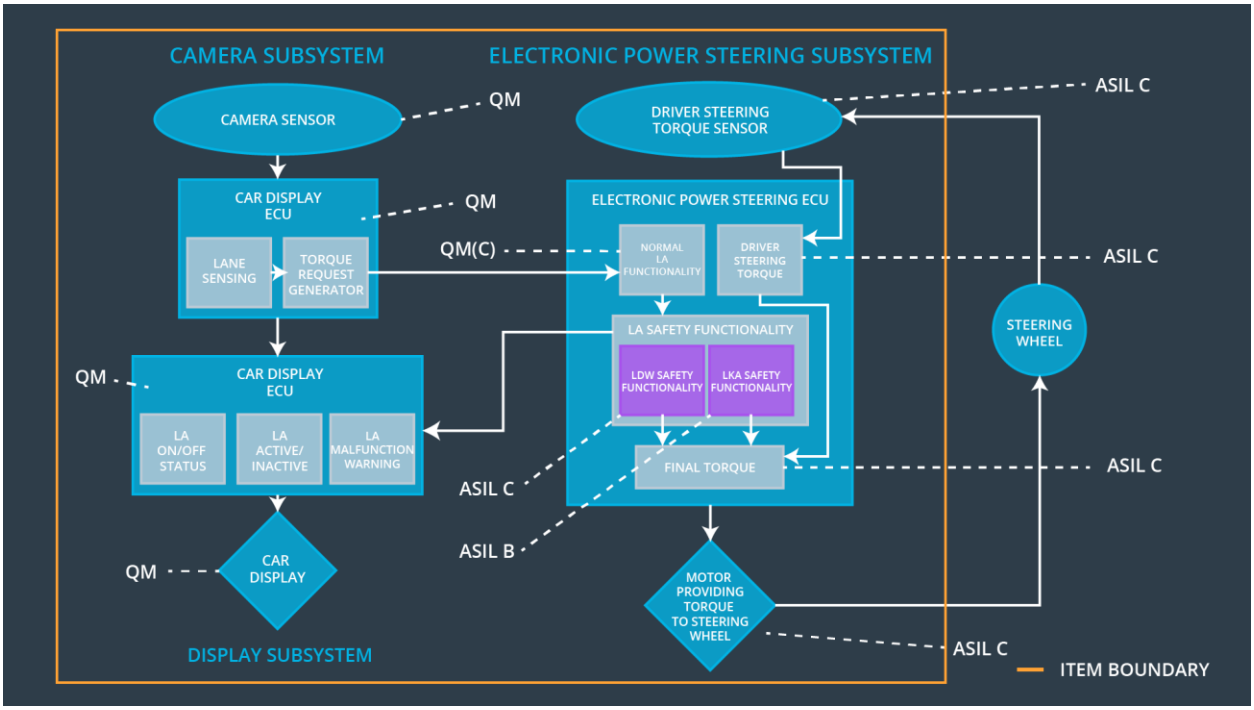
[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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 oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Torque is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Frequency is below Max_Torque_Frequency

Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is 0.

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?]

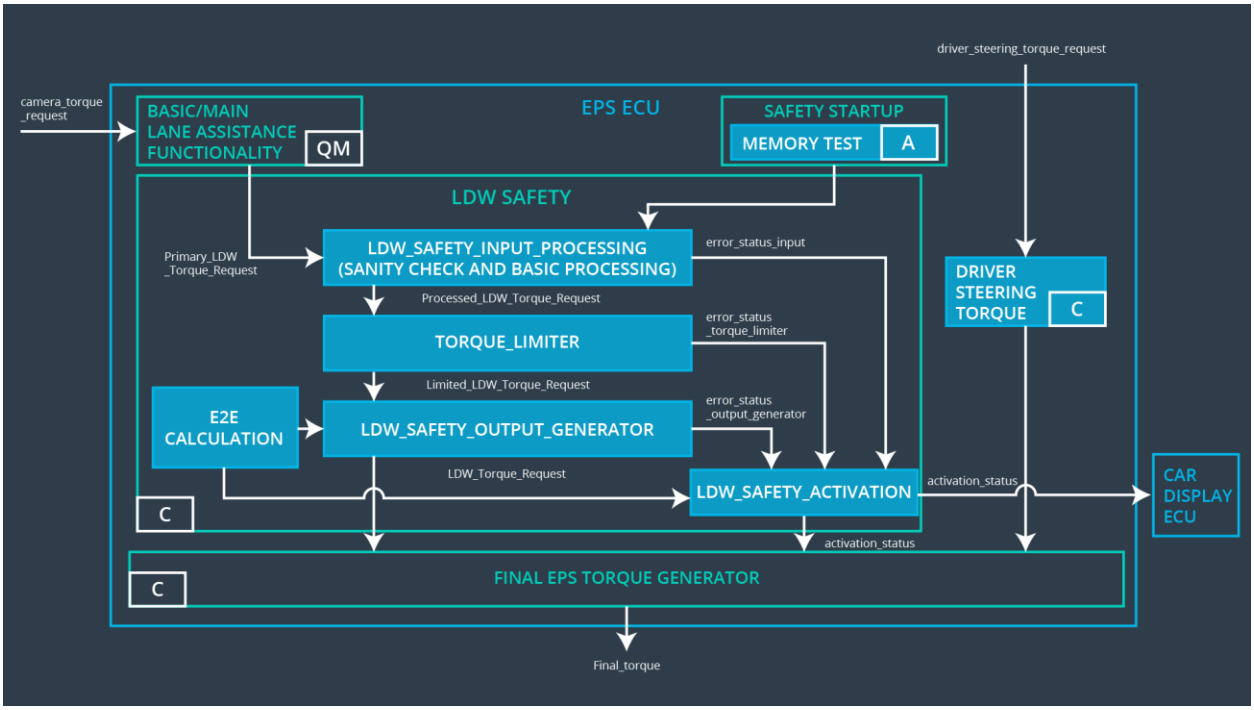
Element	Description
Camera Sensor	takes images of the road and passes it to

	Camera Sensor ECU
Camera Sensor ECU - Lane Sensing	detects lane lines and lane departures
Camera Sensor ECU - Torque request generator	calculates the required torque and sends the request to Electronic Power Steering ECU and sends warning to Car Display ECU
Car Display	displays warnings and status of Lane Departure Assistance to driver
Car Display ECU - Lane Assistance On/Off Status	shows the status of lane assistance functionality
Car Display ECU - Lane Assistant Active/Inactive	shows if the lane assistance functionality is active or not
Car Display ECU - Lane Assistance malfunction warning	shows warning if there is a malfunction in lane assistance functionality
Driver Steering Torque Sensor	measures the turning of the steering wheel by the driver
Electronic Power Steering (EPS) ECU - Driver Steering Torque	receives and analyzes the torque provided by the driver.
EPS ECU - Normal Lane Assistance Functionality	receives warning from Camera Sensor ECU and torque request.
EPS ECU - Lane Departure Warning Safety Functionality	ensures torque amplitude is below Max_Torque_Amplitude and torque frequency is below Max_Torque_Frequency
EPS ECU - Lane Keeping Assistant Safety Functionality	ensures Lane Keeping Assistance functionality is not active more than Max_Duration time.
EPS ECU - Final Torque	passes final torque to steering motor by combining Lane Keeping torque request and Lane Departure Warning functionalities.
Motor	provides the torque indicated by the Electronic Power Steering ECU 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	The lane keeping item shall	X		

Requirement 01-01	ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude			

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' component is below 'Max_Torque_Amplitude.'	C	50 ms	Lane Departure Warning Safety	Lane Departure Warning torque set to zero.
Technical Safety Requirement 02	As soon as the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	Lane Departure Warning Safety	Lane Departure Warning torque set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_Torque_Request' to zero.	C	50 ms	Lane Departure Warning Safety	Lane Departure Warning torque 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 to

					zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for faults in memory.	A	Ignition cycle	Safety Startup	Lane Departure Warning torque 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	The Lane Departure Warning safety component shall ensure that the frequency of the	C	50 ms	Lane Departure Warning	Lane Departure

01	'LDW_Frequency_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.'			Safety	Warning frequency set to zero.
Technical Safety Requirement 02	As soon as the Lane Departure Warning is deactivated, the 'LDW Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	Lane Departure Warning Safety	Lane Departure Warning frequency set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the Lane Departure Warning functionality, it shall deactivate the Lane Departure Warning feature and set 'LDW_ Frequency _Request' to zero.	C	50 ms	Lane Departure Warning Safety	Lane Departure Warning frequency set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_ Frequency_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Departure Warning frequency to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for faults in memory.	A	Ignition cycle	Safety Startup	Lane Departure Warning frequency to zero.

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

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 safety component shall ensure that the duration of the 'LKA_Duration_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Duration.'	C	50 ms	Lane Keeping Assistance Safety	Lane Keeping Assistance torque set to zero.
Technical Safety Requirement 02	As soon as the Lane Keeping Assistance is deactivated, the 'LKA Safety' software module shall send a signal to the Car Display ECU to turn on a warning signal.	C	50 ms	Lane Keeping Assistance Safety	Lane Keeping Assistance torque set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the Lane Keeping Assistance functionality, it shall deactivate the Lane Keeping Assistance feature and set 'LKA_ Duration _Request' to zero.	C	50 ms	Lane Keeping Assistance Safety	Lane Keeping Assistance torque set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_ Duration_Request' signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Keeping Assistance torque set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for faults in memory.	A	Ignition cycle	Safety Startup	Lane Keeping Assistance torque set to zero.

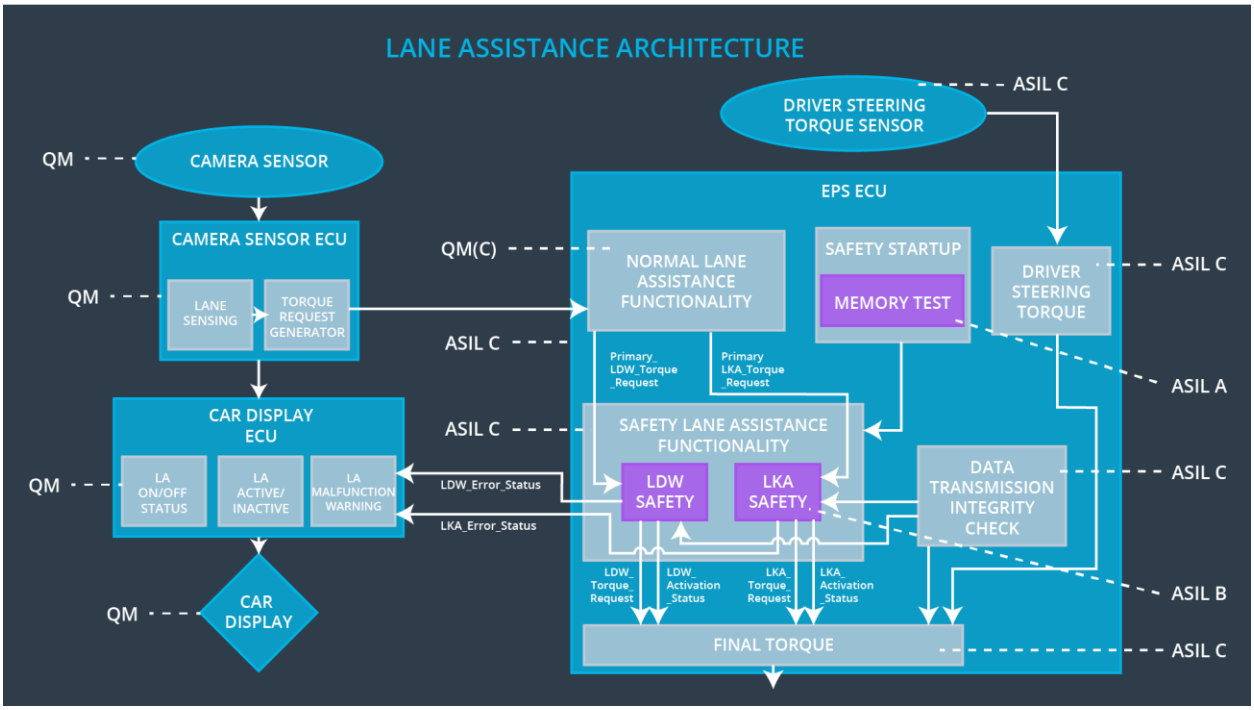
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right

answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

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 are allocated to the Electronic Power Steering ECU.

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 Lane Departure Warning functionality	Malfunction_01, Malfunction_02	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display