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
22-11-2017	1.0	Pablo Elizalde	First draft
28-11-2017	1.1	Pablo Elizalde	Fixed technical safety requirements table

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 Technical Safety Concept is a more concrete document and gets more into details of the item's technology. It belongs to the product development level of the V Model. It defines how the subsystems interact at the message level and describes how the ECUs communicate with each other.

Inputs to the Technical Safety Concept

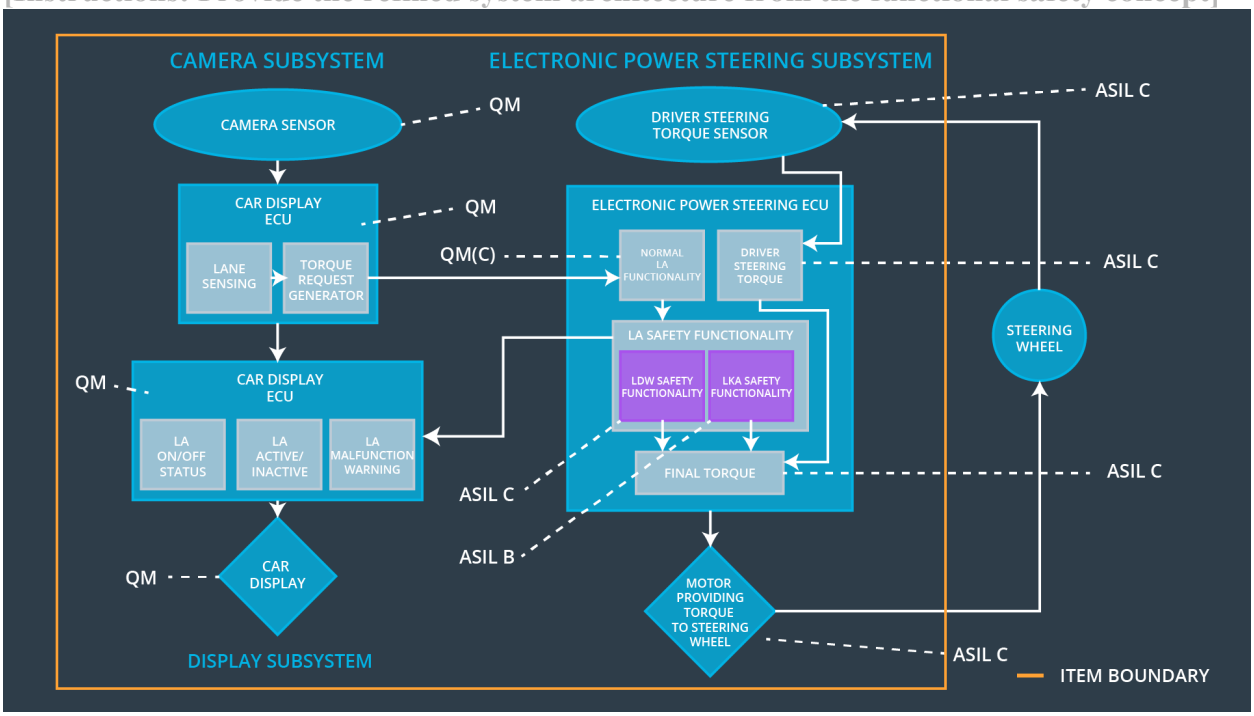
Functional Safety Requirements

[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 EPS ECU shall ensure that the lane departure warning torque amplitude is below is Max_Torque_Amplitude.	C	50ms	Turn the system off.
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure warning torque frequency is below is Max_Torque_Frequency.	C	50ms	Turn the system off.
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	Turn the system off.

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 in images from the road.
Camera Sensor ECU - Lane Sensing	The ‘Lane Sensing’ from the Camera Sensor ECU detects if the car is driving out of the ego lane and pass the information to the ‘Torque request generator’.
Camera Sensor ECU - Torque request generator	The ‘Torque request generator’ receives the information from the ‘Lane Sensing’ and request to apply a torque to the ‘Electronic Power Steering

	ECU' if needed.
Car Display	The car display shows to the user information coming from the Car Display ECU.
Car Display ECU - Lane Assistance On/Off Status	It decides if the LA status is On or Off depending on the information received from the Camera Sensor ECU.
Car Display ECU - Lane Assistant Active/Inactive	It decides if the LA in active or inactive depending on the information received from the Camera Sensor ECU.
Car Display ECU - Lane Assistance malfunction warning	It decides to if is needed to display a warning signal to the user based on the output of the 'LA Safety functionality'.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor informs to the Electronic Power Steering ECU about the amount of torque that the driver is applying.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The 'Driver Steering Torque' receives the input from the 'Driver Steering Torque Sensor' and sends the information to the 'Final Torque'.
EPS ECU - Normal Lane Assistance Functionality	The 'Normal Lane Assistance' receives information from the 'Torque Request Generator' and calculates the vibrational torque request.
EPS ECU - Lane Departure Warning Safety Functionality	The 'Lane Departure Warning Safety Functionality' receives the vibrational torque request from the 'Normal Lane Assistance' and makes sure that is below the maximum amplitude and frequency. If is above it will deactivate the functionality and inform the 'Car Display ECU'.
EPS ECU - Lane Keeping Assistant Safety Functionality	The 'Lane Keeping Assistant Safety Functionality' makes sure that the torque steering assistance is no longer than the 'Max_Duration'. If is longer it will deactivate the functionality and inform the 'Car Display ECU'.
EPS ECU - Final Torque	The 'Final Torque' receives request from each safety functionality together with the 'Driver Steering Torque'
Motor	The motor is in charge to provide the torque coming from 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 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	The LDW safety component shall ensure that the amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic	C	50ms	LDW Safety Functionality	LDW shall set the oscillating torque to 0.

01	power steering Torque' component is below 'Max_Torque_Amplitude.				
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 Functionality	LDW shall set the oscillating torque to 0.
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 Functionality	LDW shall set the oscillating torque to 0.
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	LDW shall set the oscillating torque to 0.
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	Safety Startup	LDW shall set the oscillating torque to 0.

[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	The lane keeping item shall	X		

Safety Requirement 01-02	ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency			

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 Functionality	LDW shall set the oscillating torque to 0.
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 Functionality	LDW shall set the oscillating torque to 0.
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 Functionality	LDW shall set the oscillating torque to 0.
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	LDW shall set the oscillating torque to 0.
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	Safety Startup	LDW shall set the oscillating torque to 0.

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.]

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Choose a reasonable value for Max_Torque_Amplitude.	Verify that the signal 'LDW_Torque_Request' does not exceed the 'Max_Torque_Amplitude'.
Technical Safety Requirement 02	Choose a reasonable value for Max_Torque_Amplitude.	Verify a signal is sent to the car display ECU to turn on a warning light when the torque amplitude crosses the limit.
Technical Safety Requirement 03	Choose a reasonable value for Max_Torque_Amplitude.	Verify that the signal 'LDW_Torque_Request' is zero.
Technical Safety Requirement 04	Choose a reasonable value for Max_Torque_Amplitude.	Verify that the signal 'LDW_Torque_Request' value sent by the LDW Safety Functionality is the same that the one received for the Final Torque.
Technical Safety Requirement 05	Choose a reasonable value for Max_Torque_Amplitude.	Verify there is no memory fault.

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 assisted torque of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' component is below ‘Max_Duration’.	B	500ms	LKA Safety Functionality	LKA shall set the oscillating torque to 0.
Technical Safety Requirement 02	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 Functionality	LKA shall set the oscillating torque to 0.
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 Functionality	LKA shall set the oscillating torque to 0.
Technical Safety Requireme	The validity and integrity of the data transmission for LKA _Torque_Request' signal shall be ensured.	B	500ms	Data Transmission Integrity Check	LKA shall set the oscillating torque to 0.

nt 04					
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	Safety Startup	LKA shall set the oscillating torque to 0.

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

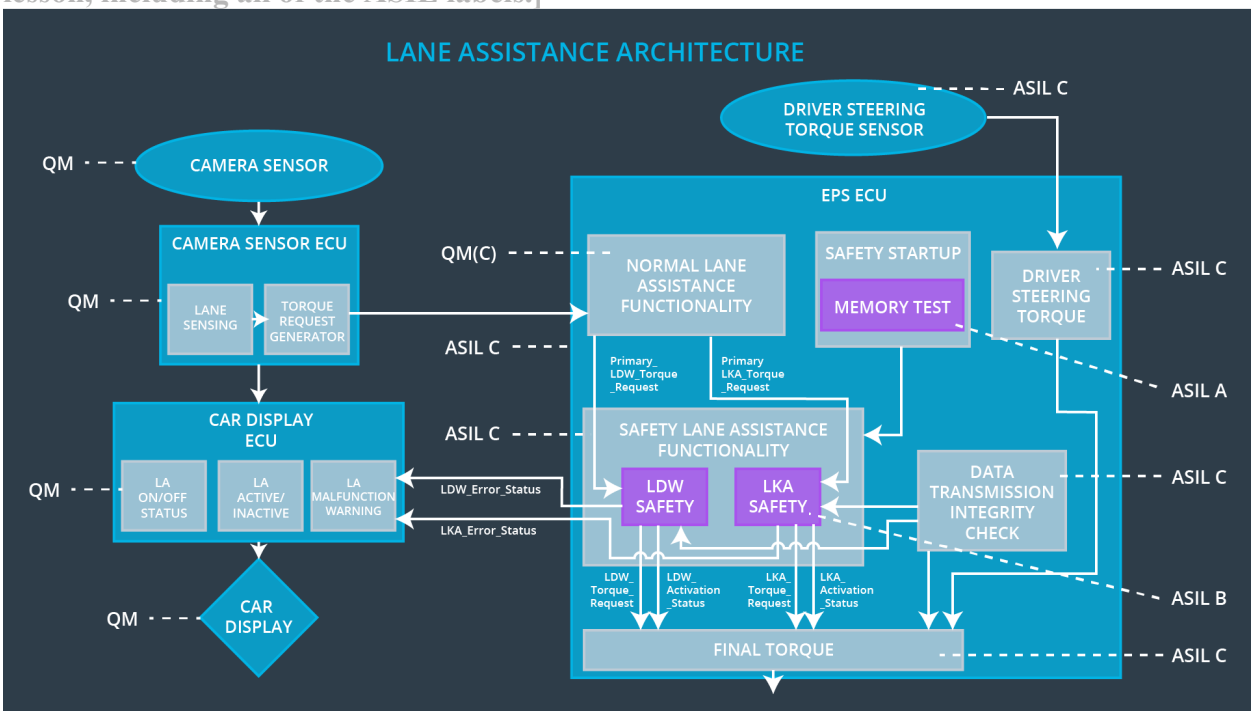
[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. "Validation" asks whether or not you chose the appropriate parameters. "Verification" involves testing to make sure the vehicle behaves as expected when the parameter value is crossed.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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Choose a reasonable value for Max_Duration.	Verify that the signal 'LKA_Torque_Request' duration not exceed the 'Max_Duration'.
Technical Safety Requirement 02	Choose a reasonable value for Max_Duration.	Verify a signal is sent to the car display ECU to turn on a warning light when the torque amplitude crosses the limit.
Technical Safety Requirement 03	Choose a reasonable value for Max_Duration.	Verify that the signal 'LKA_Torque_Request' is zero.
Technical Safety Requirement 04	Choose a reasonable value for Max_Duration.	Verify that the signal 'LKA_Torque_Request' value sent by the LKA Safety Functionality is the same that the one received for the Final Torque.

Technical Safety Requirement 05	Choose a reasonable value for Max_Duration.	Verify there is no memory fault.

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 our technical safety requirements are allocated in the Electronic Power Steering ECU. Most of the requirements are related with the LDW and LKA functionality, that is why those requirements are allocated in the LDW Safety Functionality and LKA Safety functionality respectively.

The other two requirements are to check the data integrity transmission and memory test and are located in the Data Transmission Integrity Check and in the Safety Startup.

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 functionality	The torque oscillation is applied is above Max_Torque_Amplitude or Max_Torque_Frecuency.	Yes	A light in the dashboard.
WDC-02	Turn off functionality	The driver keeps its hands off the wheel for a longer time than Max_Duration.	Yes	A light in the dashboard.