



Elektrobit



UDACITY

Functional 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
20/11/2018	1	Omar	First attempt

Table of Contents

[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. 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 Functional Safety Concept](#)

[Inputs to the Functional Safety Analysis](#)

[Safety goals from the Hazard Analysis and Risk Assessment](#)

[Preliminary Architecture](#)

[Description of architecture elements](#)

[Functional Safety Concept](#)

[Functional Safety Analysis](#)

[Functional Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Functional Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

Purpose of the Functional Safety Concept

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

The purpose of functional safety concept avoiding accidents by reducing risk to acceptable levels

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

[Instructions:

REQUIRED:

Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

OPTIONAL:

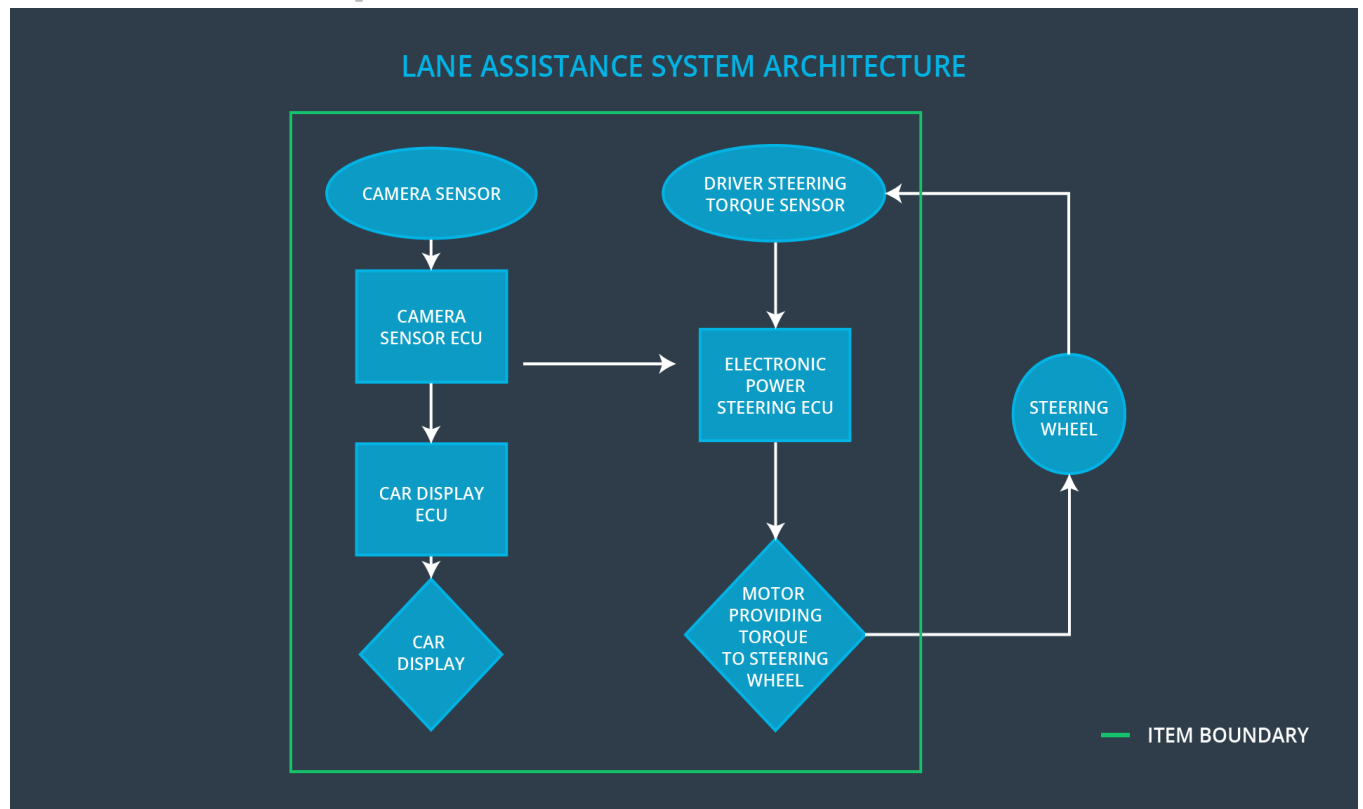
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.

]

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited
Safety_Goal_02	The lane keeping assistance function shall be time limited, and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]



Description of architecture elements

[Instructions: Provide a description for each of the item elements; 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	Camera Sensor ECU ensure torque request amplitude is below maximum and id
Car Display	Display the output of the system to the driver
Car Display ECU	Car Display ECU controls a light that tells the driver If the lane keeping item is on or off and second one will Control a light telling the driver that the lane departure Warning is activated
Driver Steering Torque Sensor	Driver Steering Torque Sensor will sense the applied

	steering of the diver on the steering wheels.
Electronic Power Steering ECU	Electronic Power Steering ECU will sense how Much the driver is turning the steering wheel and t will receive the vibrational torque request from the camera Subsystem this is where we will limit the amplitude and The frequency to be low max torque amplitude and max torque frequency. the last thing Electronic Power Steering ECU do it will add these torque request together to output a final torque to the motor that moves the steering wheel.
Motor	Motor will Providing torque to steering

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

[Instructions: Fill in the functional safety analysis table below.]

Malfunction ID	Main Function of the Item Related to Safety Goal Violations	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting Malfunction
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude
Malfunction_02	Lane Departure	MORE	

	Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback		The lane departure warning function applies an oscillating torque with very high torque frequency
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.

Functional Safety Requirements

[Instructions: Fill in the functional safety requirements for the lane departure warning]

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	A S I L	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane departure warning torque request amplitude shall be set to zero
Functional	The lane keeping item shall ensure that the	C	50 ms	Lane departure

Safety Requirement 01-02	lane departure oscillating torque frequency is below Max_Torque_Frequency			warning torque request amplitude shall be set to zero
--------------------------	---	--	--	---

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	For whatever value we end up choosing for the max torque amplitude, we need to validate that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value.	Once we have validated our choice, we then need to verify that the safety requirement is met; when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.
Functional Safety Requirement 01-02	For whatever value we end up choosing for the max torque frequency, we need to validate that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value.	Once we have validated our choice, we then need to verify that the safety requirement is met; when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what

		happens.
--	--	----------

[Instructions: Fill in the functional safety requirements for the lane keeping assistance]

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
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	lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving

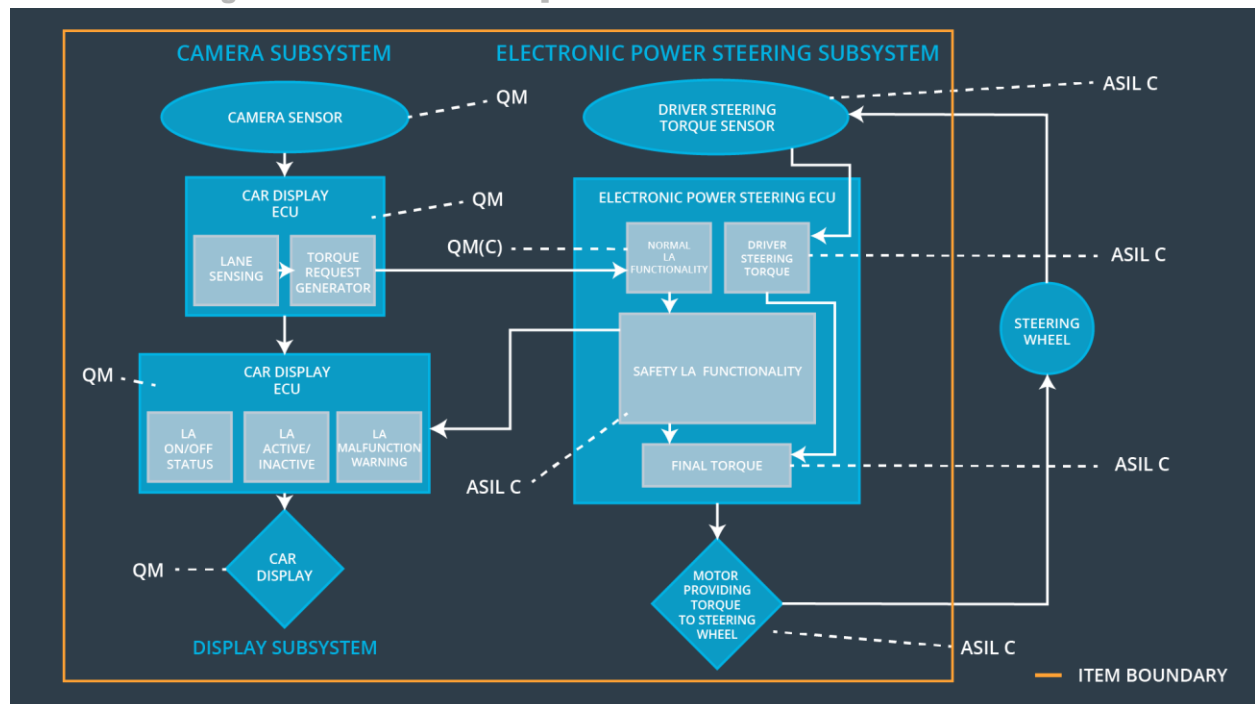
Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
----	---	---

Functional Safety Requirement 02-01	For the lane keeping assistance function, we would have to test and validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel	Then we would verify that the system really does turn off if the lane keeping assistance every exceeded max_duration.
-------------------------------------	---	---

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 functional safety lesson including all of the ASIL labels.]



Allocation of Functional Safety Requirements to Architecture Elements

[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01		Yes	No	No
Functional Safety Requirement 01-02		Yes	No	No
Functional Safety Requirement 02-01		Yes	No	No

Warning and Degradation Concept

[Instructions: Fill in the warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the functionality	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	Yes	There is no warning
WDC-02	turn off the functionality	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in	Yes	the driver will see a warning light on the

		order to stay in ego lane		dashboard when the system malfunction s
--	--	------------------------------	--	---