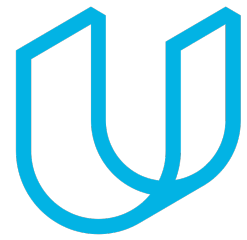




Elektrobit



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
4/04/2018	1.0	Adam shan	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?]

Functional safety looks at what happens when the system does something that it was not supposed to do, which is called a malfunction and the purpose of functional safety concept are Identifying hazards and evaluating the risk and lowering risk to reasonable 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:

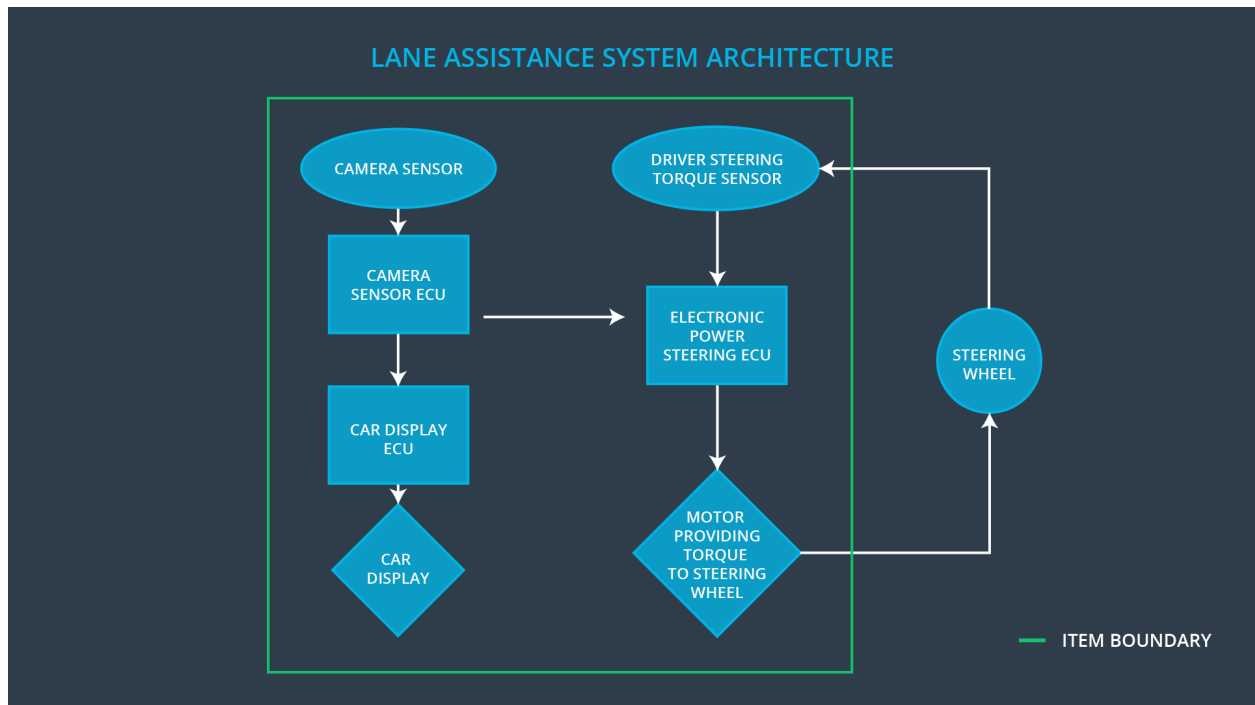
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.

]

ID	Safety Goal
Safety_Goal_01	The oscilling torque to the steering wheel from the lane keeping assistance 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	Collecting data for Camera Sensor ECU
Camera Sensor ECU	Lane sensing and torque request generator
Car Display	Display system and warning information from Car Display ECU
Car Display ECU	Display lane assistance on/off status and whether lane assistance is active
Driver Steering Torque Sensor	Collecting data and analyze driver steering torque
Electronic Power Steering ECU	Lane assistance functionality and final electronic power steering torque output
Motor	Providing torque to steering wheel

# 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 (above limit)
Malfunction_02	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 frequency (above limit)
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	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping item shall ensure that the lane departure oscilling torque amplitude is below Max_Torque_Amplitude.	C	50 ms	LDW will set the oscilling torque amplitude to 0.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscilling torque frequency is below Max_Torque_frequency.	C	50 ms	LDW will set the oscilling torque amplitude to 0.

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	validate that we chose a reasonable value.	test how drivers react to different torque amplitudes and frequencies to prove that we chose an appropriate value.
Functional Safety Requirement 01-02	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.

[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	The lane keeping item shall ensure that the	C	50 ms	the lane

Safety Requirement 02-01	lane keeping assistance torque is applied for only Max_Duration			assistance system should stop applying extra torque after a certain amount of time.
--------------------------	---	--	--	---

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	test and validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	the electronic power steering ECU shall ensure that limit torque amplitude is below		

		Max_Torque_ amplitude.		
Functional Safety Requirement 01-02	The line keeping item shall ensure that the lane departure oscilling torque frequency is below Max_Torque_frequency.	the electronic power steering ECU shall ensure that limit torque frequency is below Max_Torque_f requency.		
Functional Safety Requirement 02-01	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	the electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration		

## 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	to turn off the functionality	The malfunctions in the lane departure warning function	YES	Display a warning on the driver dashboard.
WDC-02	to turn off the functionality	The malfunctions in the lane keeping assistance	YES	Display a warning on the driver dashboard.



		function.		
--	--	-----------	--	--