



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
03/10/18	1.0	Franz Pucher	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](#)

## Purpose of the Functional Safety Concept

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

## 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:**

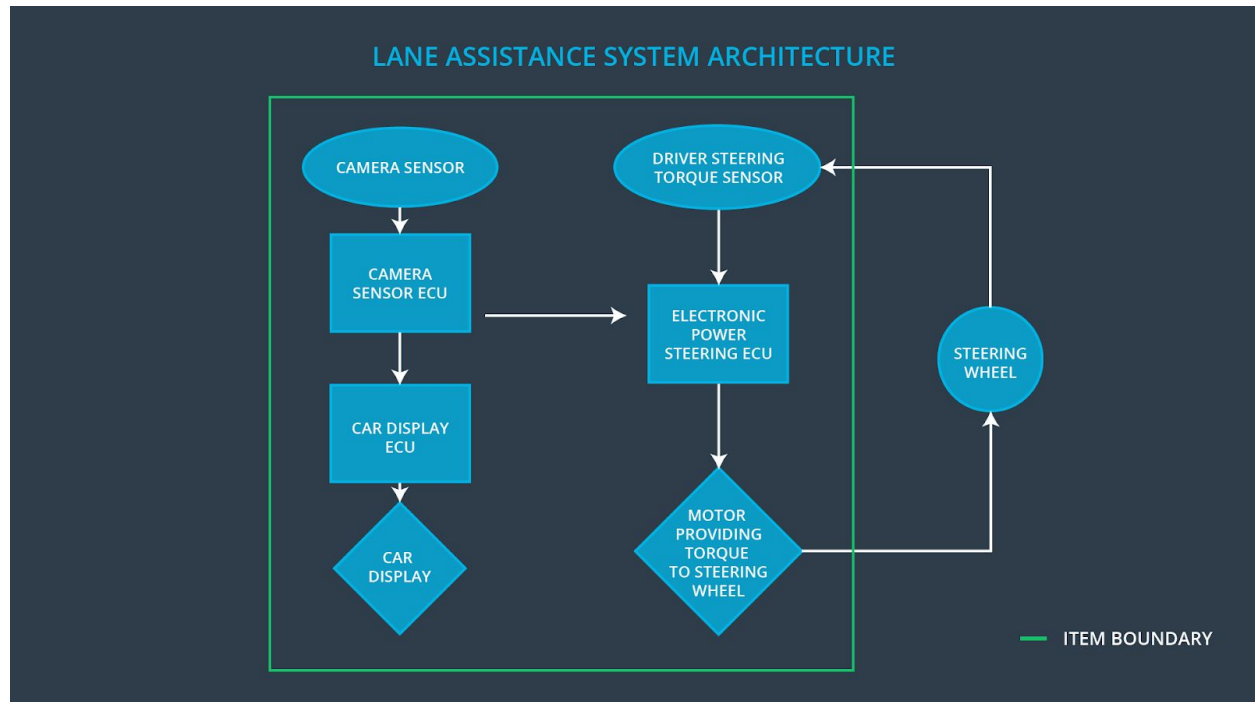
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.

]

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 image from the road.
Camera Sensor ECU	The camera sensor ECU identifies when the vehicle has accidentally departed its lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	This subsystem signals an active lane assistance item and in case of warnings. When the driver is leaving the lane without using the indicator a warning is displayed. It relies on the signals from its ECU
Car Display ECU	This subsystem signals an active lane assistance item and in case of warnings. When the driver is leaving the lane without using the indicator a warning is displayed. It uses the Car Display to inform the driver.
Driver Steering Torque Sensor	Provides sensor readings of the driver torque, which

	are used in the Electronic Power Steering ECU.
Electronic Power Steering ECU	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. It relies on a driver steering torque sensor and the motor providing torque to the steering wheel.
Motor	Provides a torque to the steering wheel in order to warn the driver by vibrating slightly. Additionally a corrective course to the center of the lane can be achieved through this motor.

## 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	MORE	The lane departure warning function applies an oscillating

	an oscillating steering torque to provide the driver a haptic feedback		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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Vibration torque is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Vibration torque is below Max_Torque_Frequency

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety	Validate that the vibration warning amount is neither too high for a driver to	Verify the system does turn off if the Lane Departure Warning exceeded

Requirement 01-01	handle nor too low that the driver cannot feel the vibration.	Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.

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

Lane Keeping Assistance (LKA) Requirements:

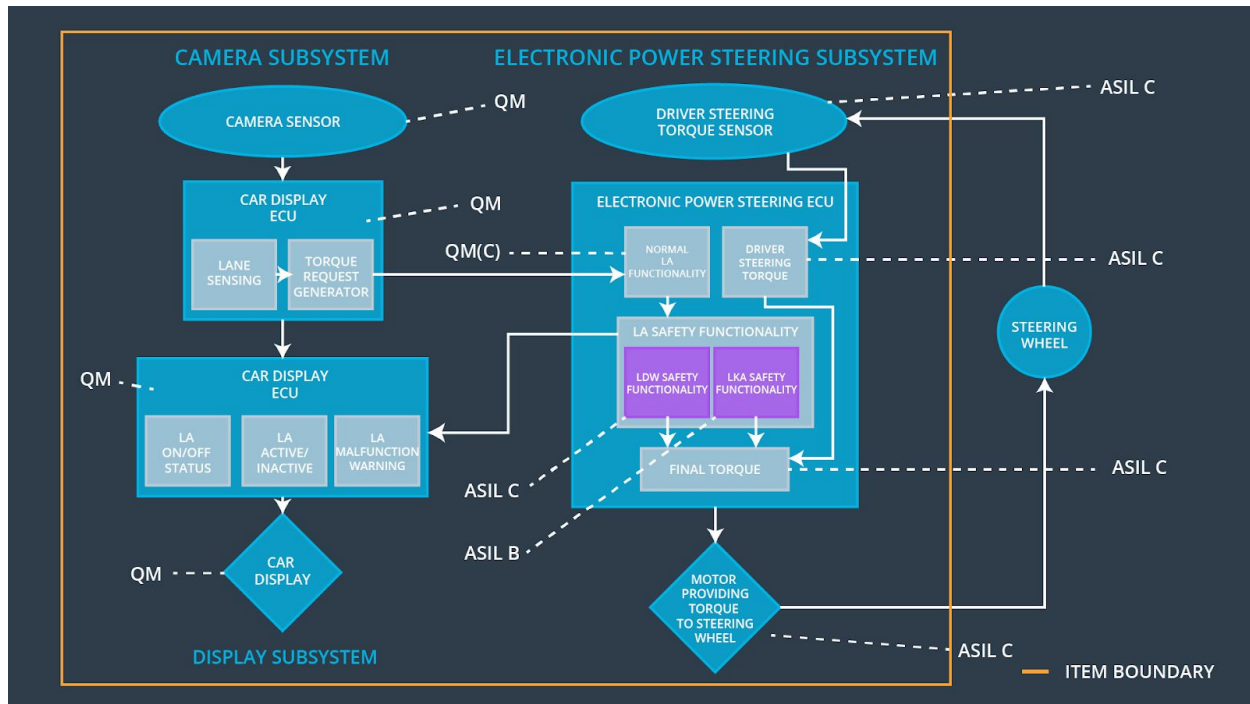
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	50 ms	Lane Keeping Assistance torque is zero.

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	Validate the Max_Duration chosen not allow the driver to use the car as self-driving car.	Verify the system does deactivate if the Lane Keeping Assistance torque application 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	x		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	x		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane keeping assistance torque is	x		



02-01	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	Turn off the functionality	The lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)	Yes	The driver will see a warning light on the dashboard when the system malfunctions
WDC-02	Turn off the functionality	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	Yes	The driver will see a warning light on the dashboard when the system malfunctions