



Elektrobit



UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
16/5/2018	1	Aakash Gupta	This is the first attempt to complete the document

Table of Contents

[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

On the Functional Safety Concept documents the system high level requirements are identified. These requirements are allocated to different parts of the item architecture. Technical safety requirements will be derived from these safety concepts. Instruction on how to validate and verify the requirements are presented as well.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

1. Lane Departure Warning:

Problem:



Safety Goal:

The oscillating steering torque from the lane departure warning function shall be limited.

2. Lane Keeping Assistance:

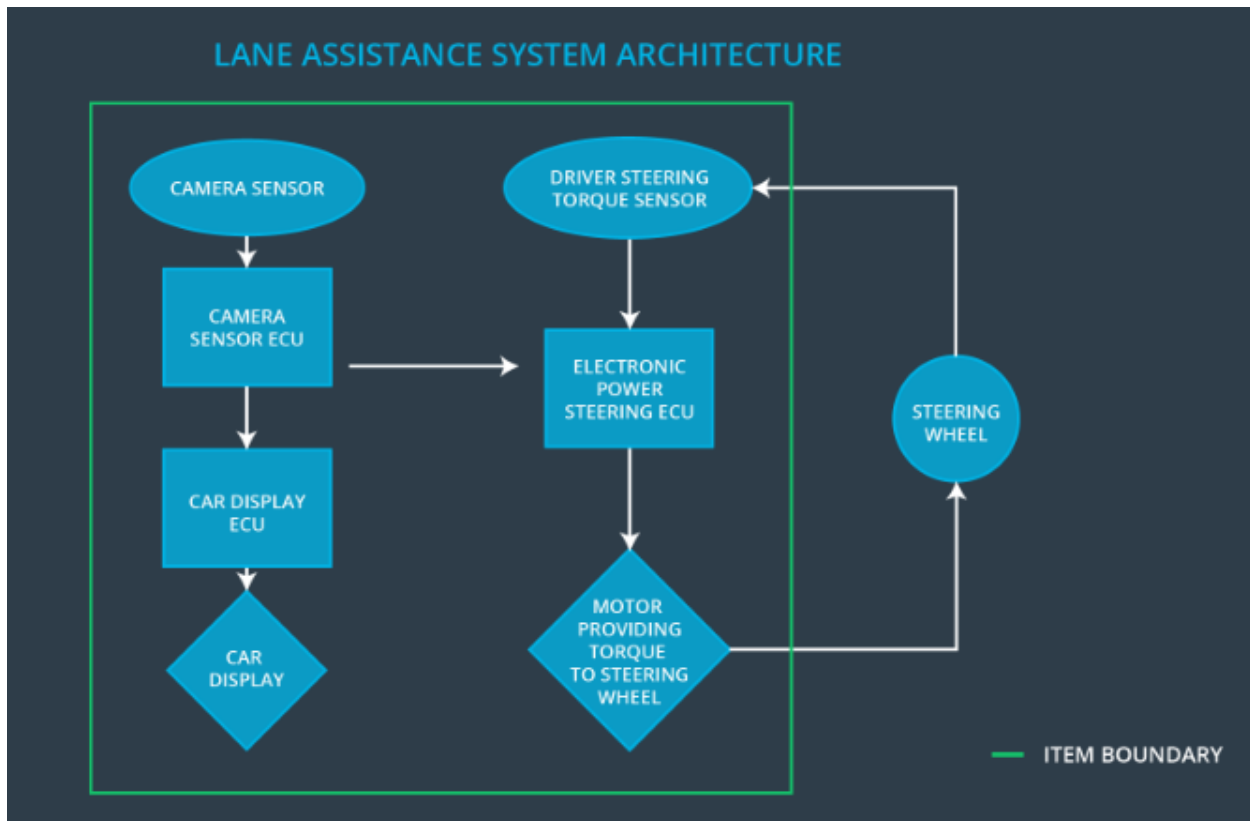
Safety Goal:

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.

OPTIONAL:

ID	Safety Goal
Safety_Goal_01	The lane keeping assistance function should only be activated if driver has at least one hand on steering and it should not just deactivate if driver leaves both the hands for 1-2 seconds.

Preliminary Architecture



Here, item is the lane assistance system.

The item boundary is drawn to include three sub-systems:

- Camera system
- Electronic Power Steering system
- Car Display system

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	Keeps track of the lane and detects lane departures.
Camera Sensor ECU	Has the hardware and software required for deep learning or for computer vision techniques like the Hough transform.
Car Display	Displays warning light on display dashboard. It can also be used to display lane departure status.
Car Display ECU	Drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	Measure torque applied to steering wheel by the driver.
Electronic Power Steering ECU	Send signal to motor for turning the steering wheel by calculating from the values received from Driver Steering Torque Sensor and from lane keeping and warning system.
Motor	Apply the torque to steering wheel according to the Electronic Power Steering ECU.

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.]

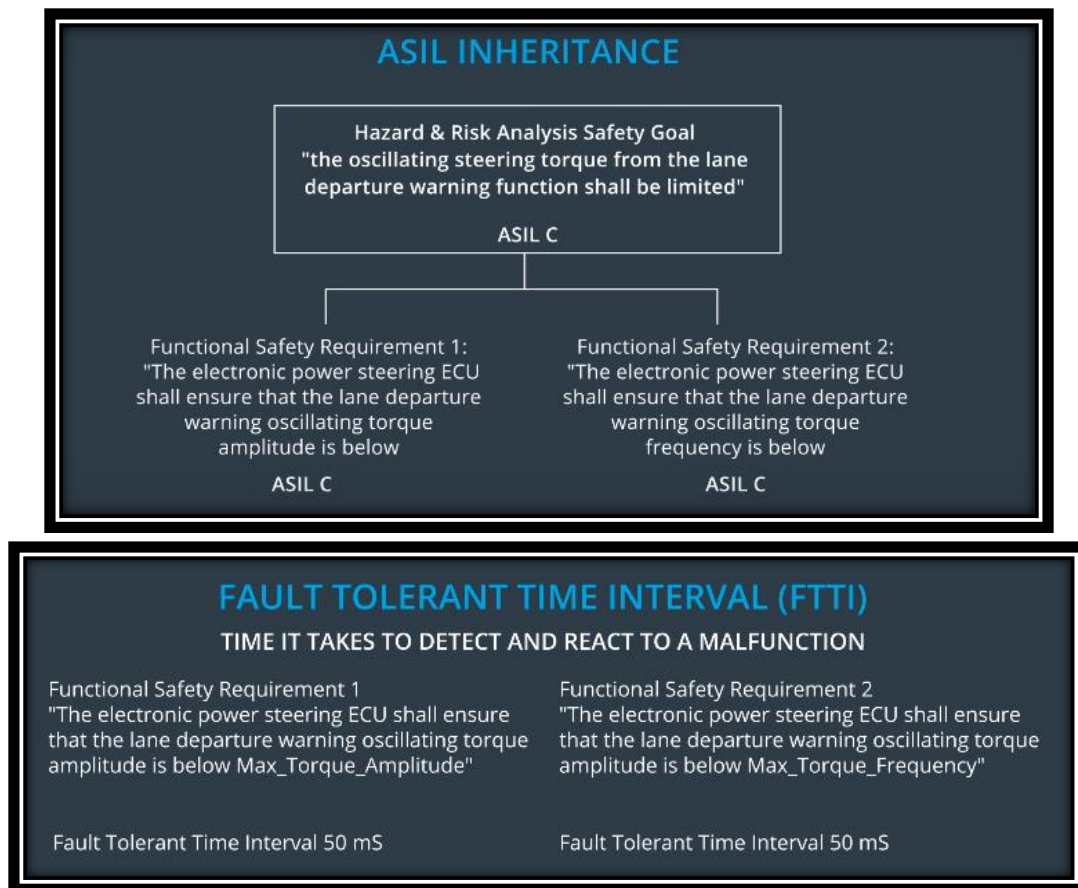
Malfunction ID	Main Function of the Item Related to Safety Goal Violations	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting Malfunction
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The Lane Departure Warning function applies an oscillating torque with very high torque frequency (above Max_Torque_Frequency)
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 amplitude (above Max_Torque_Amplitude)
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 lead to misuse as an autonomous driving function

Functional Safety Requirements

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 amplitude 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 amplitude below Max_Torque_Frequency

Reference for above table:



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	To validate that we chose a reasonable value we can conduct test how drivers react to different torque amplitudes. Hence proving that we chose an appropriate value.	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. We can do a software test inserting a fault into the system and see if system turns off.
Functional Safety Requirement 01-02	To validate that we chose a reasonable value we can conduct test how drivers react to different torque frequencies. Hence proving that we chose an appropriate value.	When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. We can do a software test inserting a fault into the system and see if system turns off.

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

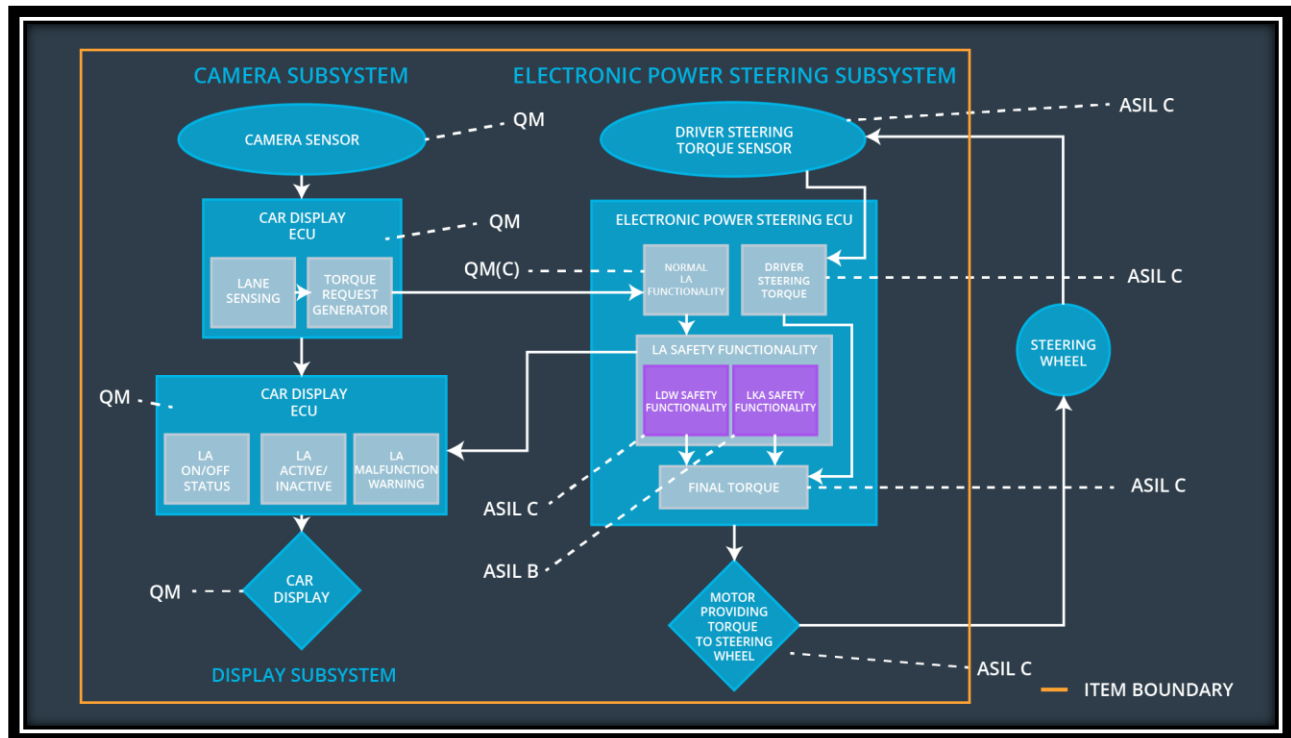
Lane Keeping Assistance (LKA) Requirements:

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 only Max_Duration.	B	500ms	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



Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	To validate that we chose a reasonable value we can conduct test how drivers react to different torque amplitudes. Hence proving that we chose an appropriate value.			
Functional Safety Requirement 01-02	To validate that we chose a reasonable value we can conduct test how drivers react to different torque frequencies. Hence proving that we chose an appropriate value.			
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.			

Warning and Degradation Concept

WDC-01: lane departure warning function

WDC-02: lane keeping assistance function

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off functionality	When oscillating time is greater than Max_Allowed_Time	Yes	Driver will see a warning light on the dashboard when the system malfunctions
WDC-02	Turn off functionality	When oscillating torque amplitude is higher than Max_Torque_Amplitude and When oscillating torque frequency is more than Max_Torque_Frequency	Yes	Driver will see a warning light on the dashboard when the system malfunctions