



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
23/05/2018	1.0	Krishna	1 st version of Functional Safety Concept

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

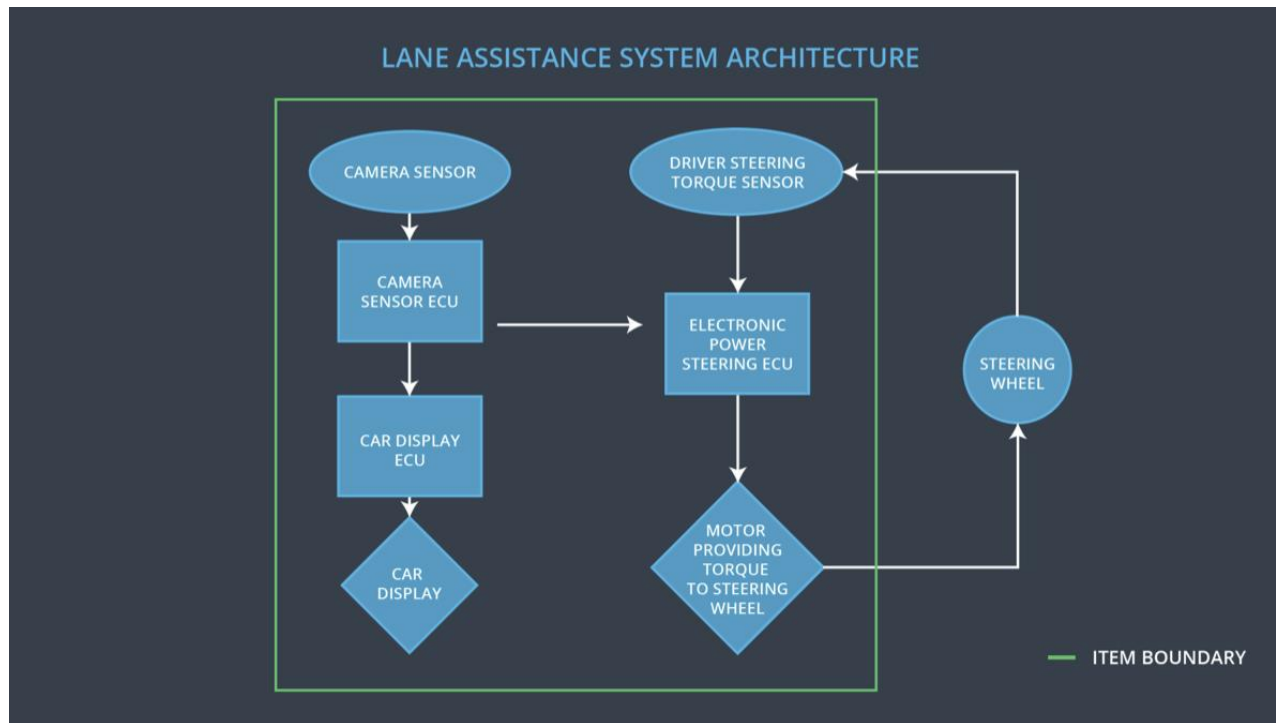
The main purpose of the Functional Safety Concept is to refine the Safety Goals, identify new requirements and allocate these requirements. Using the concept from Hazard Analysis and Risk Assessment, it tries to identify the requirements to lower the risk levels. It evaluates the risk of the hazardous situation so that we know how much we need to lower the risk. The functional safety concepts lead to Technical Safety Concept.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	It takes visual feedback for the lane detection. It captures images and feeds the images to the Camera Sensor ECU
Camera Sensor ECU	It analyses the camera images using computer vision or some other techniques. It determines whether the car is going out of the lane. It sends this information to the Car Display system as well as power steering ECU
Car Display	It displays whether the lane keeping and departure assistance system is on/off. So, basically it is a visual feedback for the driver.
Car Display ECU	Generates warning signals depending upon the input from the camera sensor ECU and Electronic Power Steering ECU to pass it to the Car Display.
Driver Steering Torque Sensor	It measures the amount of torque being applied on the steering wheel and sends it to the Electronic Power Steering ECU

Electronic Power Steering ECU	Processes inputs from the camera sensor ECU, driving steering torque sensor and generates appropriate Lane Assistance functionality. Sends the output to the motor.
Motor	It is the component which actually applies the torque to rotate the 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

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 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
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

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	Lane Assistance is not activated
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	Lane Assistance is not activated

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 to prove 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.
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 frequency, to prove 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.

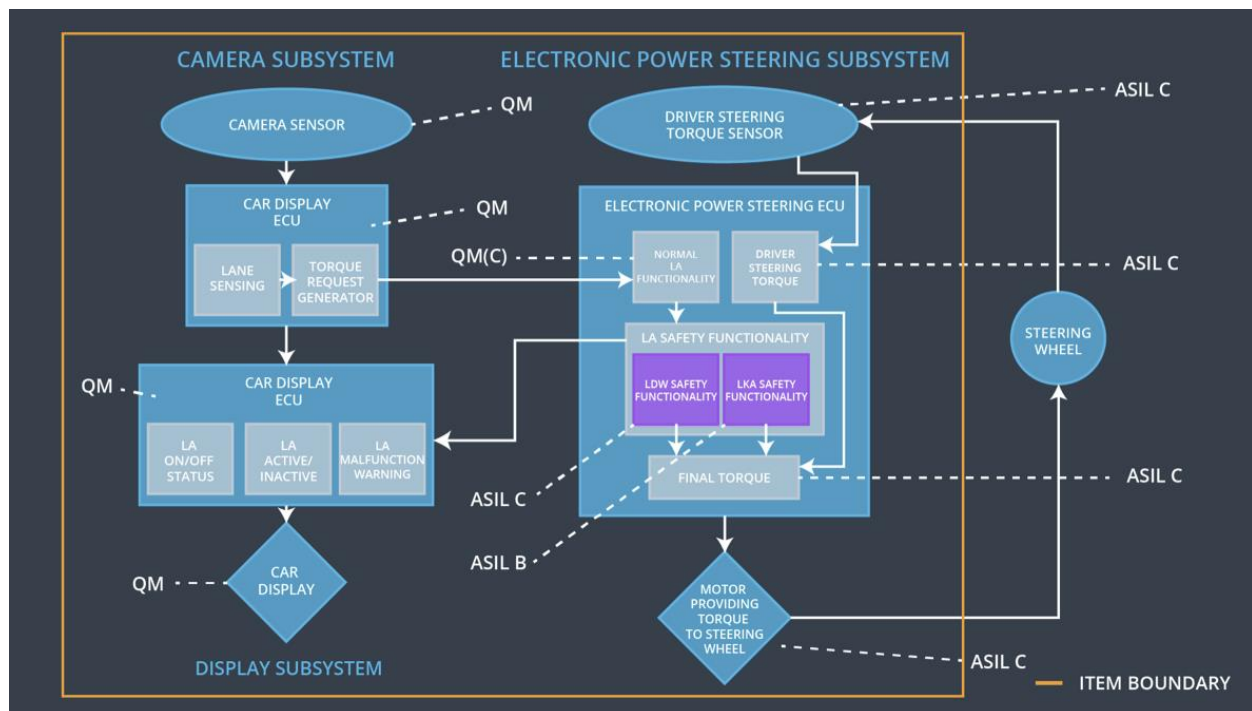
Lane Keeping Assistance (LKA) Requirements:

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 Assistance System is deactivated

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.	The system turns off if the lane keeping assistance ever 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	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	Yes	No	No
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	Yes	No	No
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	Yes	No	No

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the functionality	The malfunction of steering wheel vibrating too high or with more frequency	Yes	Display will show the warning light on
WDC-02	Turn off the functionality	The malfunction of lane keeping assistance applied for long duration	Yes	Display will show the warning on