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/May/2018	1.0	Shreya Srivastava	First Draft

Table of Contents

1. Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to refine the safety goals to the functional safety requirements and allocate the requirements to the system architecture. The functional safety concept also covers the ASIL level, fault tolerant time interval and the safe state of the system for each of the functional requirements.

2. Inputs to the Functional Safety Concept

2.1 Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning system 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 that the driver cannot misuse the system for autonomous driving.

2.2 Preliminary Architecture

The architecture of the lane assistance system has the following subsystems:

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

Description of architecture elements

Element	Description
Camera Sensor	Capture the images of the road ahead and provide to the camera sensor ECU for further analyses
Camera Sensor ECU	Analyses the images sent by the cameara sensor to make decisions
Car Display	Displays the Lane Departure System warnings

Car Display ECU	Processes the various inputs and sends the warnings of the lane departure and the lane keeping system to the car display system
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel
Electronic Power Steering ECU	Use the information form the various subsystems to request the torque to be applied to the steering wheel.
Motor	Applies the torque requested by the Electronic power steering ECU to the steering wheel.

3. Functional Safety Concept

The functional safety concept consists of:

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

3.1 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(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

3.2 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 system shall ensure that the lane departure oscillating torque amplitude is below the Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The lane Keeping shall ensure that the lane departure oscillating torque frequency is below the Max_Torque_Frquency.	C	50 ms	Vibration frequency 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	Validate if the chosen value of the	Verify that the torque amplitude

Safety Requirement 01-01	Max_Torque_Amplitude is reasonable so that the driver does not lose control on the vehicle.	to the steering wheel by the lane departure system goes down to the acceptable levels well within the fault tolerant interval
Functional Safety Requirement 01-02	Validate if the chosen value of the Max_Torque_Frequency is reasonable so that the driver does not lose control on the vehicle.	Verify that the torque frequency to the steering wheel by the lane departure system goes down to the acceptable levels well within the fault tolerant interval

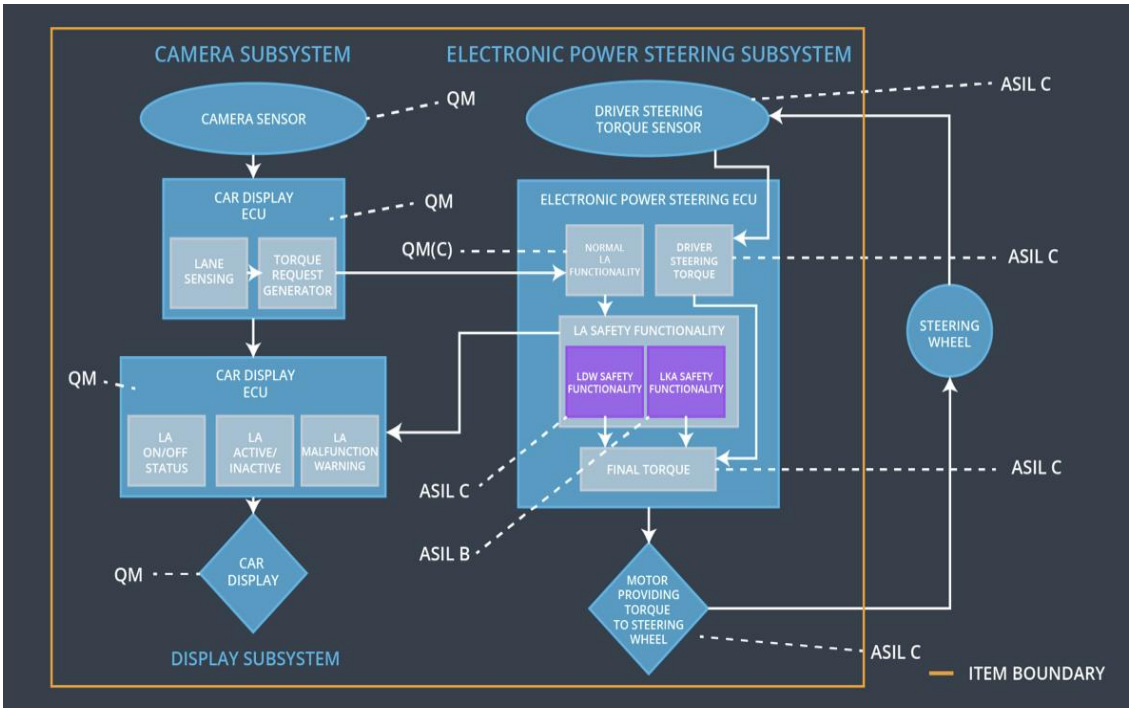
Lane Keeping Assistance (LKA) Requirements:

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 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 if the max_duration chosen for the lane keeping assistance system to switch off does not allow the driver to leave the steering wheel and use the system as a fully autonomous system.	Verify the lane keeping system shuts down after the max_duration is elapsed.

3.3 Refinement of the System Architecture



3.4 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 system shall ensure that the lane departure oscillating torque amplitude is below the Max_Torque_Amplitude.	Yes	No	No
Functional Safety Requirement 01-02	The lane Keeping shall ensure that the lane departure oscillating torque frequency is below the	Yes	No	No

	Max_Torque_Frquency.			
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

3.5 Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display