Functional Safety Concept Lane Assistance

Document Version: [Version]
Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-28-2018	0.1	majing	first draft
1-5-2018	1.0	majing	submission

Table of Contents

# Purpose of the Functional Safety Concept

The purpose of the functional safety Concept is to document the safety goals at a high level. Although it will not extend to technical details, the information from the concept will be used to create 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 so that the driver will remain alert towards the surroundings - road and traffic movement.

Preliminary Architecture
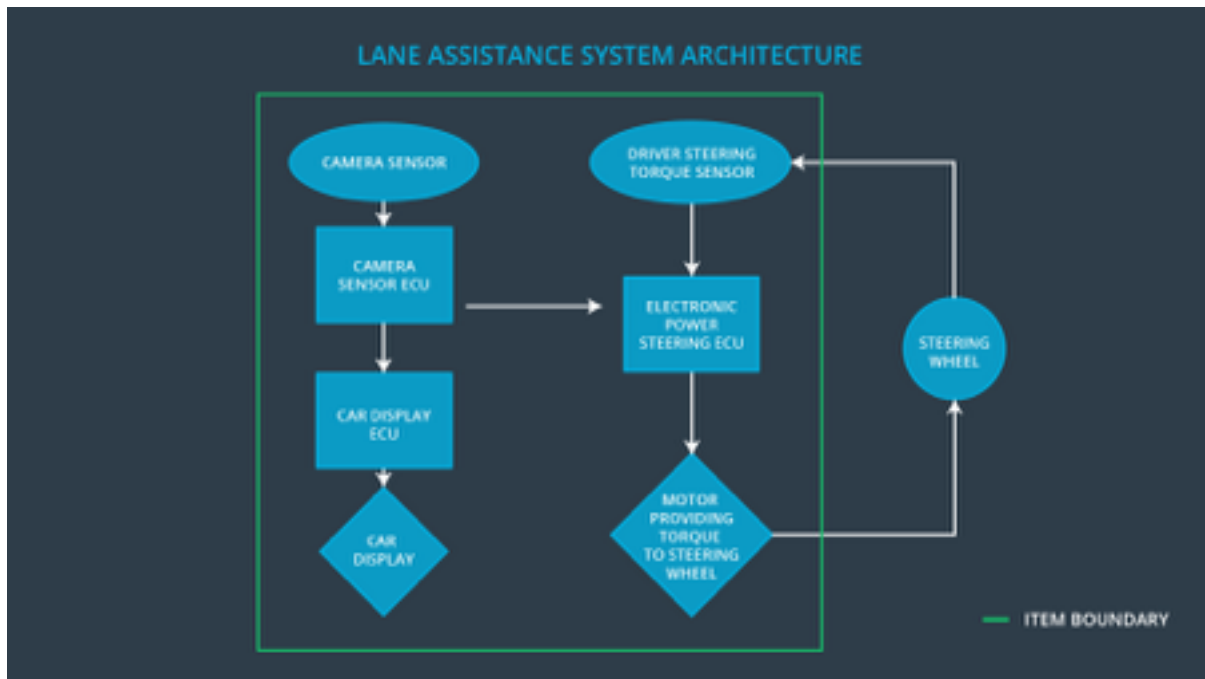
Description of architecture elements

Element	Description
Camera Sensor	Capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU	Analyse provided images to calculate the car position on the road respect to the road lanes.
Car Display	Provide feedback to the driver displaying warnings and the Lane Departure Assistance status.
Car Display ECU	Determines what information is to be shown from the driver based on the lane positioning data received from the Camera Sensor ECU.

Driver Steering Torque Sensor	Detects the current steering torque and forwards the same to the Electronic Power Steering ECU.
Electronic Power Steering ECU	Use the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning and request the necessary torque to be applied by the Motor actuator.
Motor	Applies the torque indicated boy the Electronic Power Steering ECU to 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 (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

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	The vibrational oscillating torque's amplitude 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	The vibrational oscillating torque's 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 Safety Requirement 01-01	Test that driver is able to respond to the chosen torque amplitude threshold in time.	If the Max_Torque_Amplitude value is exceeded, the system is turned off.
Functional Safety Requirement 01-02	Test that driver is able to respond to the chosen torque frequency threshold in time.	If the Max_Torque_Frequency value is exceeded, the system is turned off.

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	The torque applied by the power steering ECU after Max_Duration is 0.

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	Study driver behavior and verify they are attentive at all times.	If the LKA is active for more than the Max_Duration, the system is turned off.

Refinement of the System Architecture
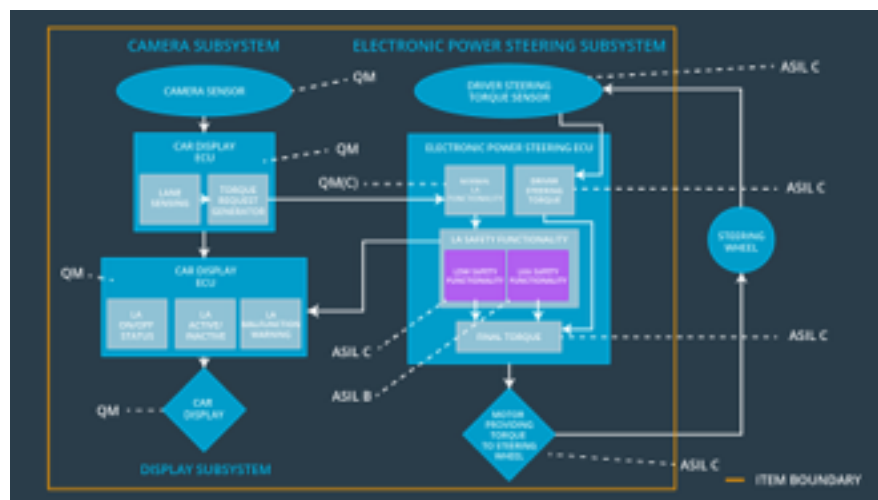
Allocation of Functional Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	x		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	x		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	x		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn system off.	Malfunction_01 Malfunction_02	Yes	Warning light on the dashboard
WDC-02	Turn system off.	Malfunction_03	Yes	Warning light on the dashboard