Functional Safety Concept Lane Assistance

Document Version: 2.0

Document history

Date	Version	Editor	Description
12/3/17	1.0	Vatche Donikian	First submission attempt
12/18/17	2.0	Vatche Donikian	Second Submission

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept is used to identify new requirements and allocate these requirements to system diagrams. This concept takes Safety goals and turns them into high-level requirements to reduce hazardous risks to acceptable levels.

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

Preliminary Architecture

The preliminary architecture of the lane assistance item consists of the camera sensor and its ECU, the car display and its ECU, the driving steering torque sensor, the electronic power steering ECU, and the motor providing torque to the steering wheel.

Description of architecture elements

Element	Description
Camera Sensor	Captures images of the road
Camera Sensor ECU	Determines when the vehicle is leaving the lane
Car Display	Lights up to notify driver of lane departure
Car Display ECU	Determines when to turn lights on in the dash
Driver Steering Torque Sensor	Determines the amount, if any, that the driver is steering
Electronic Power Steering ECU	Determines the amount of torque request to send to the motor

Motor	Provides torque 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 EPS ECU shall ensure that the lane departure warning torque amplitude is below Max_Torque_Amplitude	C	50 ms	Turn function off
Functional Safety Requirement 01-02	The EPS ECU shall ensure that the lane departure torque frequency is below Max_Torque_Frequency	C	50 ms	Turn function off

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	Choose a maximum torque amplitude, and 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 should set to zero within the 50 ms fault tolerant time interval. Perform a software test inserting a fault into the system and seeing what happens.
Functional Safety Requirement 01-02	Choose a maximum torque frequency, and test how drivers react to different torque frequencies to prove that we chose an appropriate value.	When the torque frequency crosses the limit, the lane assistance output should set to zero within the 50 ms fault tolerant time interval. Perform a software test inserting a fault into the system and seeing what happens.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State

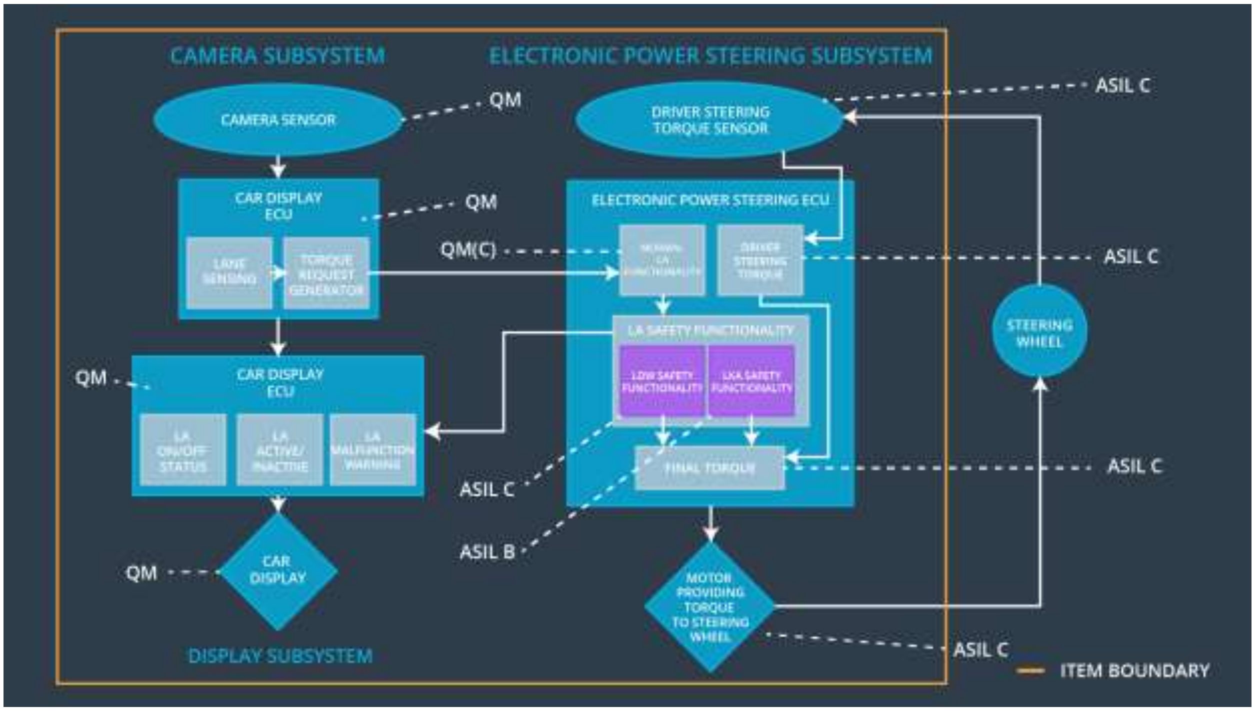
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	Turn function off

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	Define a maximum duration time for the system and then test and validate that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	Test on drivers and vehicles that the system really does turn off if the lane keeping assistance every exceeded max_duration.

Refinement of the System Architecture

The refined system architecture is shown below. Subsystem components can be classified by the ASIL score of their corresponding safety requirements. Also, the components can be split into different ASIL risk parts.



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**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	**Yes**		
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**		

Warning and Degradation Concept

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