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
20-Jan-2018	1.0	Vijayakumar K	Initial version

Table of Contents

Purpose of the Functional Safety Concept

The Functional Safety Concept documents the system high level safety requirements. These requirements are allocated to different parts of the item architecture. Technical safety requirements will be derived from these safety concepts.

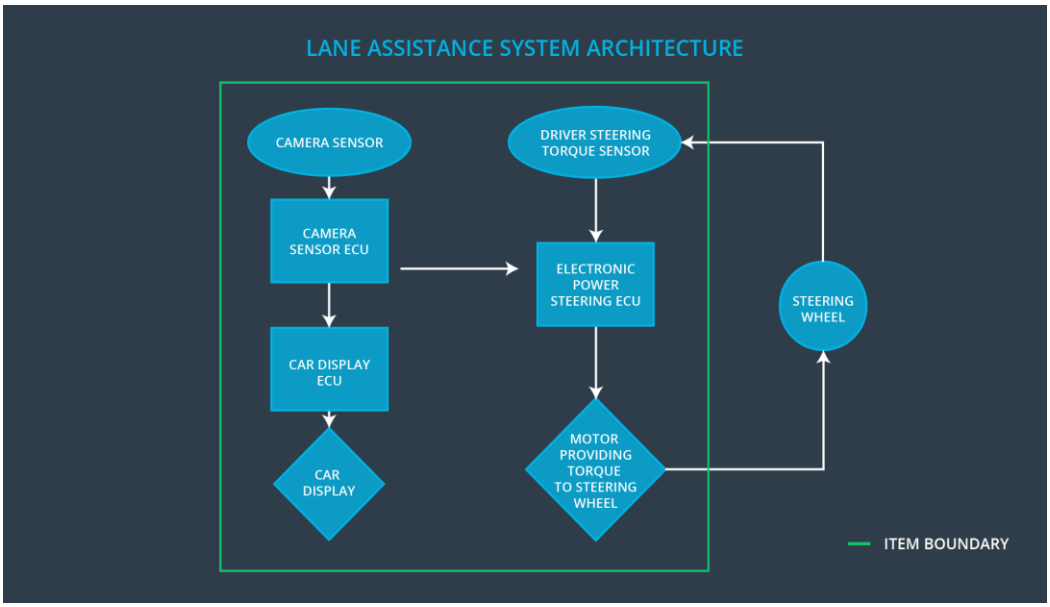
Inputs to the Functional Safety Concept

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 usage of LKS in always ON mode shall be warned to driver.
Safety_Goal_03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.

Preliminary Architecture

The basic architecture, system and the boundary is as shown below:



Description of architecture elements

Element	Description
Camera Sensor	Capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU	Analyze 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	Drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
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 by 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	MORE	The Lane Departure

	Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback		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 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 Departure Warning 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 Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	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 Safety Requirement 01-01	Validate Max_Torque_Amplitude chosen is high enough to be detected by a driver while low enough not to cause loss of steering	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.

Lane Keeping Assistance (LKA) Requirements:

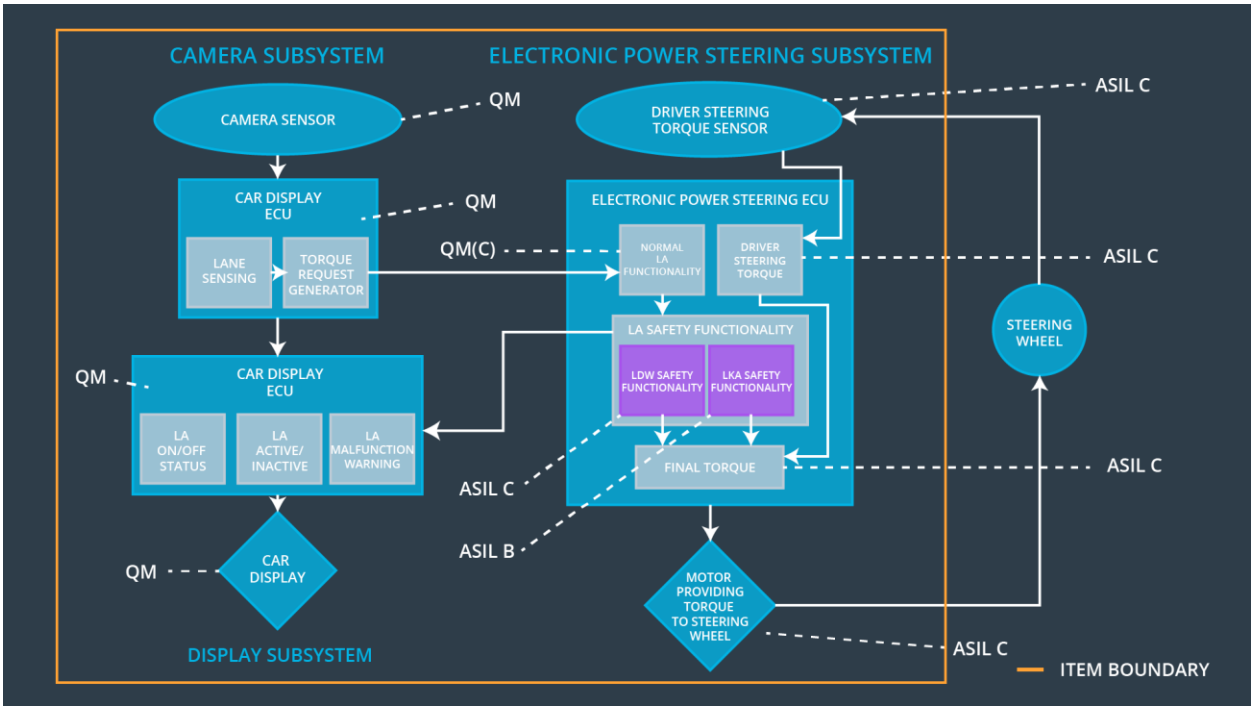
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	C	10 ms	Function 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	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.
Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the camera sensor stop working.	Verify the system does deactivate the Lane Keeping Assistance if the camera sensor is not working.

Refinement of the System Architecture

The detailed system architecture and the item boundary is as shown below:



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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety	The electronic power steering ECU shall ensure that the Lane	**X**		

Requirement 02-01	Keeping Assistance torque is applied only Max_Duration.			
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	**X**		

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, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display