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
20/06/2018	1.0	Aditya	

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 Functional Safety Concept documents the identified systems high level requirements. These requirements are allocated to different part of the item architecture. Technical safety requirements will be derived from the safety concept. The validation concept for these requirements are presented as well.

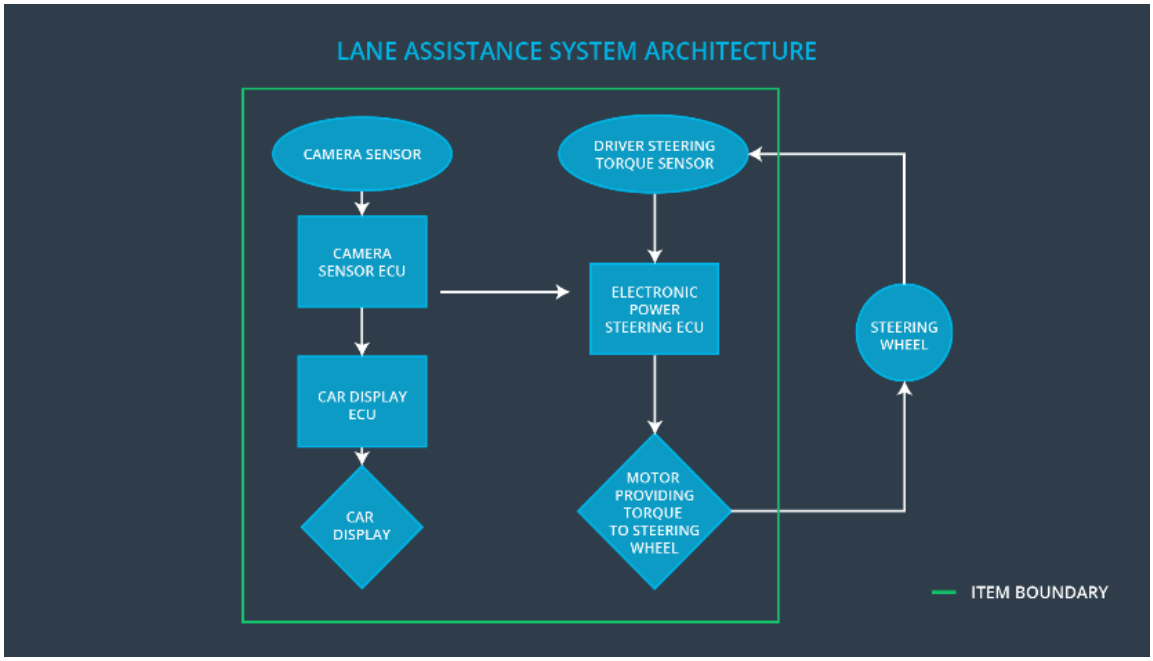
Inputs to the Functional Safety Concept

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 system is not misused for autonomous driving.
Safety_Goal_03	The lane keeping assistance function has to be deactivated if camera is not able to detect the lane lines correctly.
Safety_Goal_04	The lane keeping assistance function shall have the ability to detect lane lines of different color, and reliably detect and react merging lanes in advance.

Preliminary Architecture

The Following figure shows the preliminary architecture of Lane Assistance System-



Description of architecture elements

Element	Description
Camera Sensor	Capture images of road lanes and send it to ECU.
Camera Sensor ECU	Process the images from camera and determine car position with respect to road lanes.
Car Display	Provides warnings and the Lane Departure Assistance status.
Car Display ECU	Controls the car display to show warnings and status of all functions.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver
Electronic Power Steering ECU	Receives the torque applied by the driver on the steering wheel from Driver Steering Torque Sensor and computes appropriate final torque which is transferred to steering wheel motor.
Motor	Receives the final torque computed by Electronic Power Steering ECU and applies it 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 LDW 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 LDW 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 LKA 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 Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane Departure warning function is not activated.
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Frequency	C	50 ms	Lane Departure warning function 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	Test and validate that Max_Torque_Amplitude chosen is low enough that driver does not lose control over the car.	Verify that the system does turn off in time if Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Test and validate that Max_Torque_Frequency chosen is low enough that driver does not lose control over the car.	Verify that the system does turn off in time if Max_Torque_Frequency is exceeded.

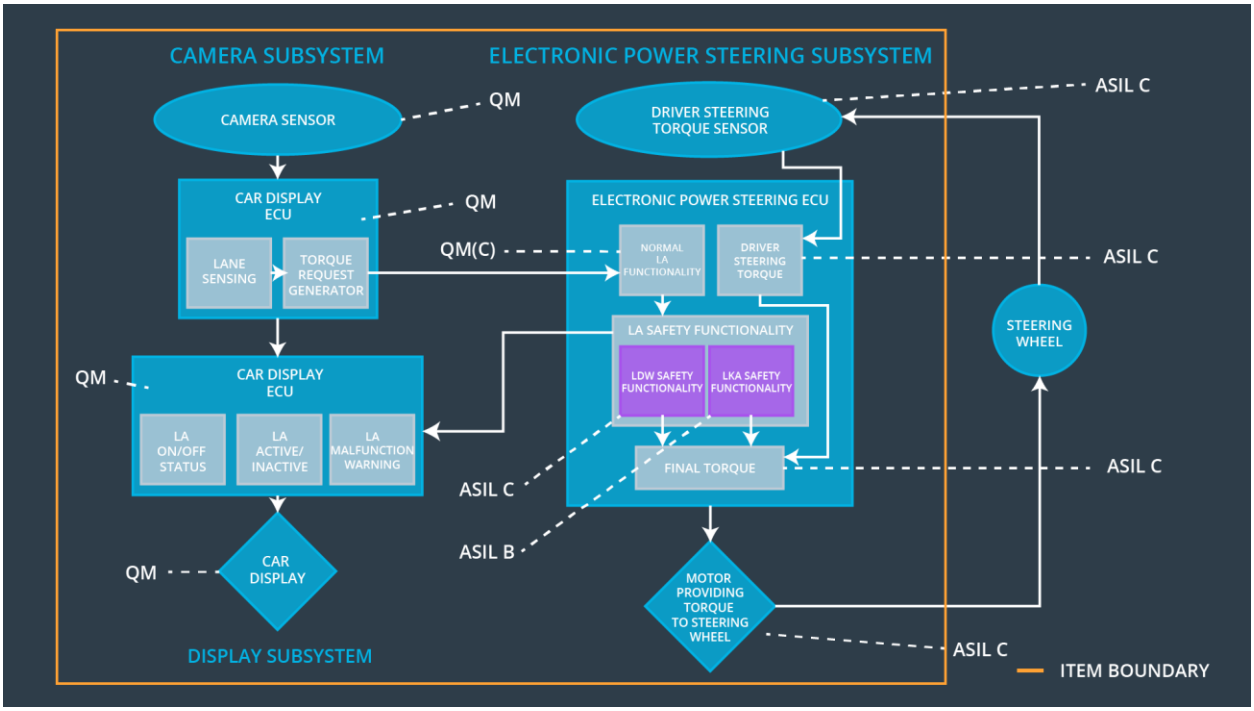
Lane Keeping Assistance (LKA) Requirements:

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 for Max_Duration.	B	500 ms	LKA is not activated.

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 Max_Duration chosen is low enough that driver does not lose control over the car	The system really does turn off if the LKA duration exceeds 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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below MAX_TORQUE_AMPLITUDE.	**Yes**	**No**	**No**
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude 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 only for 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 system	Malfunction_01 Malfunction_02	Yes	Warning light on dashboard
WDC-02	Turn off system	Malfunction_03	Yes	Warning light on dashboard