Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description

5/23/2018	1.0	Ninad K	Initial Draft
5/25/2018	1.1	Ninad K	Made changes to safety state per reviewer's comments

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 goal of the Functional Safety Concept is to document the safety goals at a high level. New requirements may be identified to meet these safety goals and allocated to the appropriate part of the system.

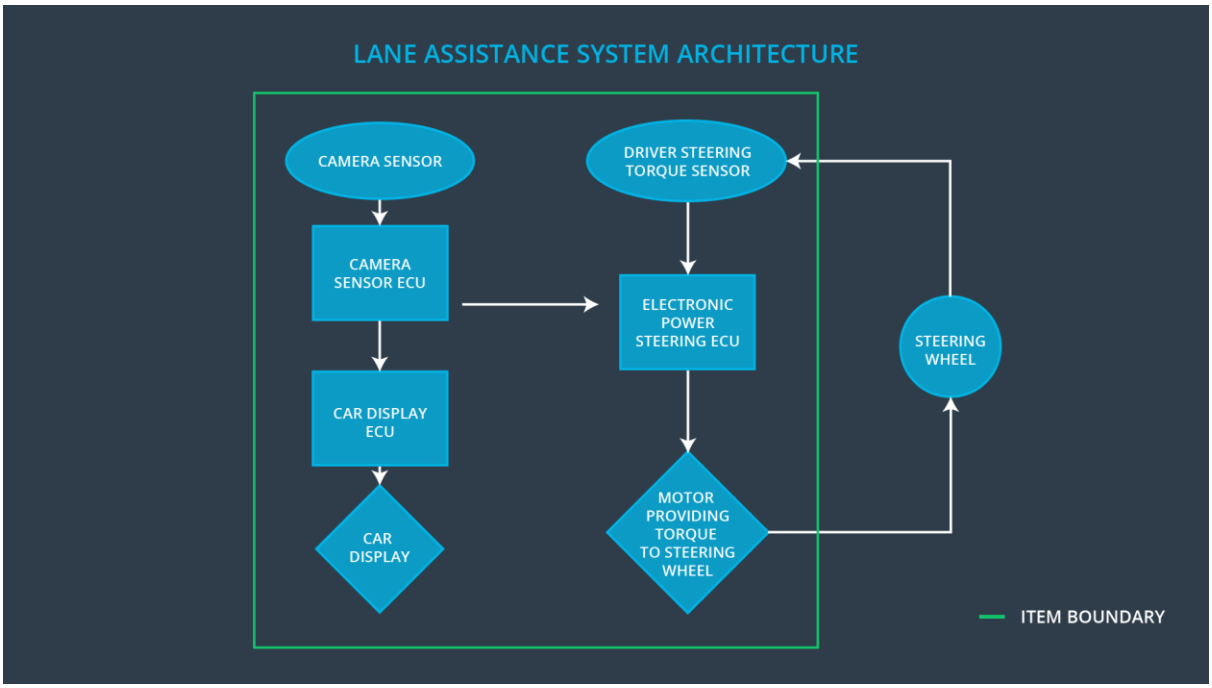
The document is restricted to the general functionality of the safety goals and does not extend to the technical details. The information from the Functional Safety Concept is used to create the Technical Safety Concept.

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	This is the vision input source and the images from this sensor are forwarded to the Camera Sensor ECU.

Camera Sensor ECU	Analyses images received from the Camera Sensor. Determines lane positioning and requests appropriate steering change from the Electronic Power Steering ECU.
Car Display	Displays warnings to the driver based on information received from the Car Display ECU.
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	Depending on the required torque and the current torque, determines the additional torque to be applied to the steering and sends the value to the motor.
Motor	Based on the data sent by the Electronic Power Steering ECU, a torque is applied to the steering.

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.

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.
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	Actual tests must be conducted with drivers to ensure that they are able to respond to the chosen torque amplitude threshold in time and appropriately.	If the Max_Torque_Amplitude value is exceeded, the system is turned off.
Functional Safety Requirement 01-02	Actual tests must be conducted with drivers to ensure that they are able to respond to the chosen torque frequency threshold in time and appropriately.	If the Max_Torque_Frequency value is exceeded, the system is turned off.

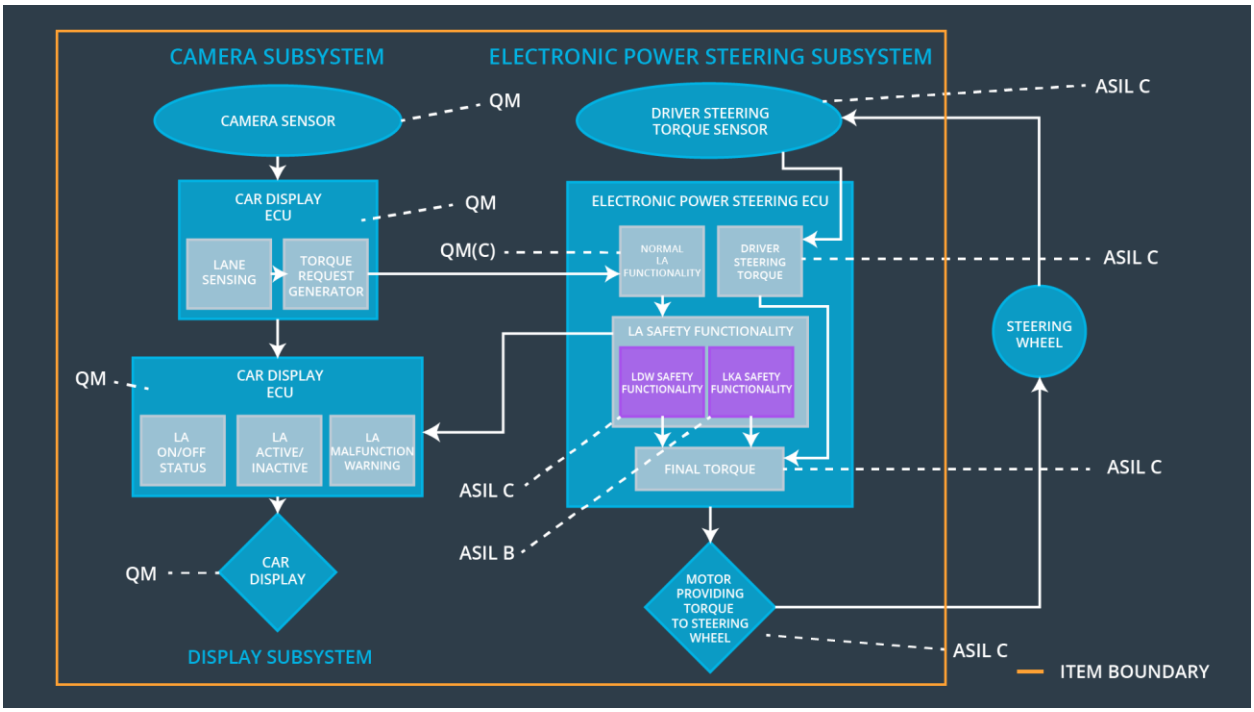
Lane Keeping Assistance (LKA) Requirements:

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	Actual driver behaviour is studied and verified to ensure that 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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane keeping item 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	Lane Assistance System is turned off.	Malfunction_01 OR Malfunction_02	Yes	Warning displayed on the Car Display.
WDC-02	Lane Assistance System is turned off.	Malfunction_03	Yes	Warning displayed on the Car Display.