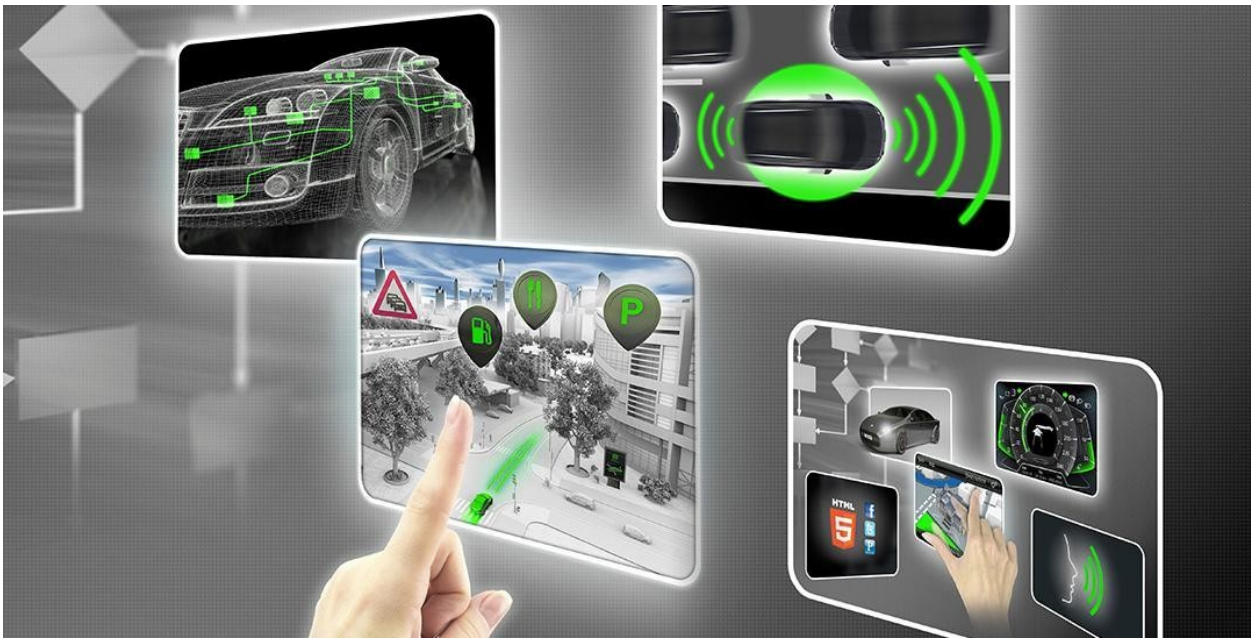
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
25/12/2018	1.0	Ahmed Desoky	Functional Safety Concept for Lane Assistance System

Table of Contents

[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Functional Safety Concept

In the functional safety concept, high level system requirements are defined. These requirements are allocated to differents parts of the system architecture. These requirements are derived from the safety goals. From the functional safety concept, we can derive technical safety requirements further on. Some details about how to validate and verify requirements are defined in this douments as well

Inputs to the Functional Safety Concept

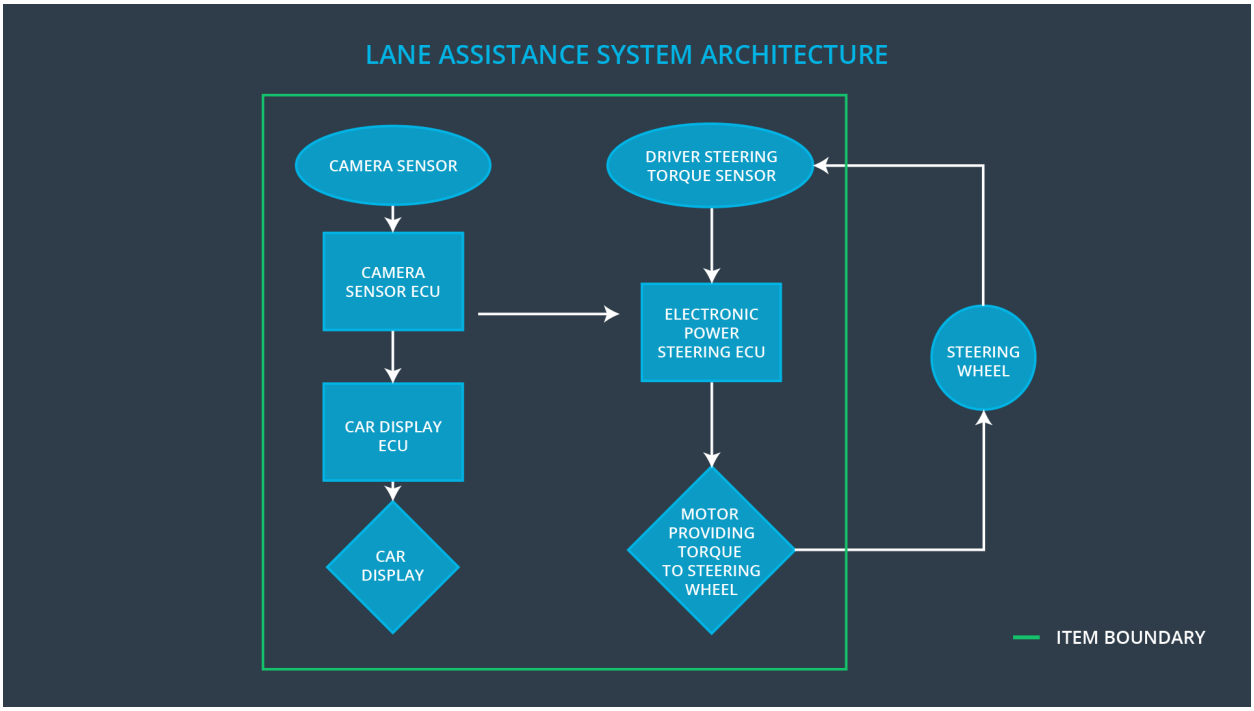
Safety goals from the Hazard Analysis and Risk Assessment

Safety goals from Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscilating steering torque from the Lane Departure Warning function shall be limited
Safety_Goal_02	The lane keepting assistance function shall be time limited as the driver may not misuse the functionality
Safety_Goal_03	The lane departure warning function shall stop when the camera sensor stops working
Safety_Goal_03	The lane keeping assistance function shall stop when the camera sensor stops working

Preliminary Architecture

The following diagram show the architecture of Lane Assistance system:



Description of architecture elements

Element	Description
Camera Sensor	Captures images and provides them to the camera ECU
Camera Sensor ECU	Processes the camera images to detect whether the vehicle is going off the lane or not
Car Display	Provides indicators for the driver to reflect the status of some systems
Car Display ECU	Takes the feedback from systems and shows the that with the proper indicator in the dashboard car display
Driver Steering Torque Sensor	Measures the toque applied to the steering wheel by the driver
Electronic Power Steering ECU	Uses the infromation from the steering torque sensor and the desired torque from the Lane Departure Warning and Lane Keep Assist to apply the torque needed to the motor
Motor	Applies the torque sent from the electrnic power steering ECU. This is the actuator

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 (LDW) function applies a torque amplitude above the limit that affects controlling the car
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 (LDW) function applies a torque frequency above the limit that affects controlling the car
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 assist is not time limited so the driver may misuse it as an autnomous car.
Malfunction_04	The lane departure warning function shall stop when the camera sensor stops working	WRONG	The lane departure warning produces random torques when the camera stops working
Malfunction_05	The lane keepring assist function shall stop when the camera sensor stops working	WRONG	The lane keeping assist produces random torques when the camera stops working

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 (LDW) shall ensure that lane departure oscillating torque is below Max_Torque_Amplitude.	C	50 ms	LDW function is deactivated
Functional Safety Requirement 01-02	The lane departure warning (LDW) shall ensure that lane departure oscillating frequency is below Max_Torque_Frequency.	C	50 ms	LDW function is deactivated
Functional Safety Requirement 01-03	The lane departure warning (LDW) shall stop when the camera sensor stops working	C	10 ms	LDW function is deactivated

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 Max_Torque_Amplitude that is sensable by any driver, while it is not leading to loss of control to the steering wheel.	Verify that the LDW function is deactivated while applying a torque amplitude > Max_Torque_Amplitude
Functional Safety Requirement 01-02	Choose Max_Torque_Frequency that is sensable by any driver, while it is not leading to loss of control to the steering wheel.	Verify that the LDW function is deactivated while applying a torque frequency > Max_Torque_Frequency
Functional Safety Requirement 01-03	Shut off the Camera while the LDW function is working	Verify the LDW function stops wokring just after the camera stops working

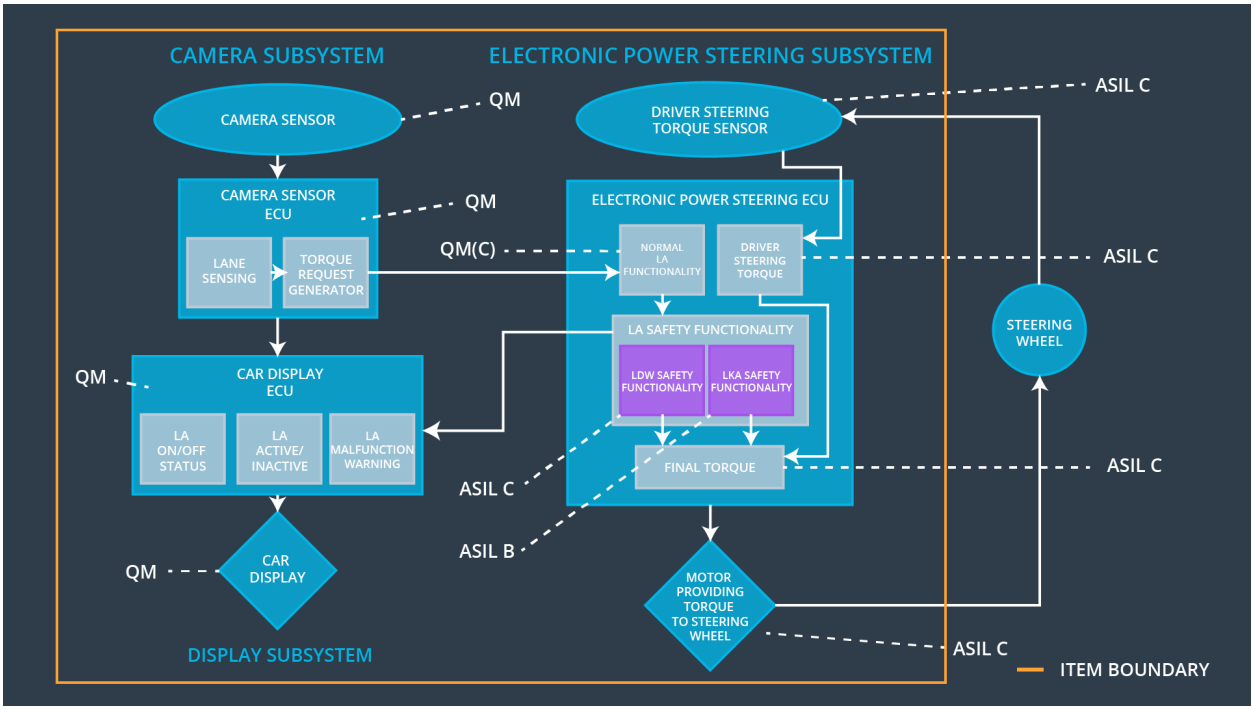
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that lane keeping assist (LKA) troque is applied for just Max_Duration	B	500 ms	LKA function is deactivated
Functional Safety Requirement 02-02	The lane keeping assist (LKA) shall stop when the camera sensor stops working	C	10 ms	LKA 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	Choose Max_Torque_Amplitude that is not giving the feeling to any driver that the car is autonomous	Verify that the LKA function is deactivated while applying a torque duration > Max_Duration
Functional Safety Requirement 02-02	Shut off the Camera while the LKA function is working	Verify the LKA function stops wokring just after the camera stops working

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 departure warning (LDW) shall ensure that lane departure oscillating torque is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane departure warning (LDW) shall ensure that lane departure oscillating frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement 01-03	The lane departure warning (LDW) shall stop when the camera sensor stops working	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that lane keeping assist (LKA) troque is applied for just Max_Duration	**X**		
Functional Safety Requirement 02-02	The lane keeping assist (LKA) shall stop when the camera sensor stops working	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the LDW	Malfunction_01, Malfunction_02, Malfunction_04	Yes	Warning indicator on the dashboard for malfunction
WDC-02	Turn off the LKA	Malfunction_03, Malfunction_05	Yes	Warning indicator on the dashboard for malfunction