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
12/12/17	1.0	Raz Nissim	Initial version

Table of Contents

Purpose of the Functional Safety Concept

A Functional Safety Concept generates actual requirements from the general functional safety goals. These are then allocated to subsystems and parts of the system. The system architecture may require modification to meet the functional safety requirements. Each of the requirements has attributes relating to the ASIL level, the fault tolerant time interval and the safe state of the system. Verification and validation of the requirements are discussed. This document does not include the technical implementation of the design.

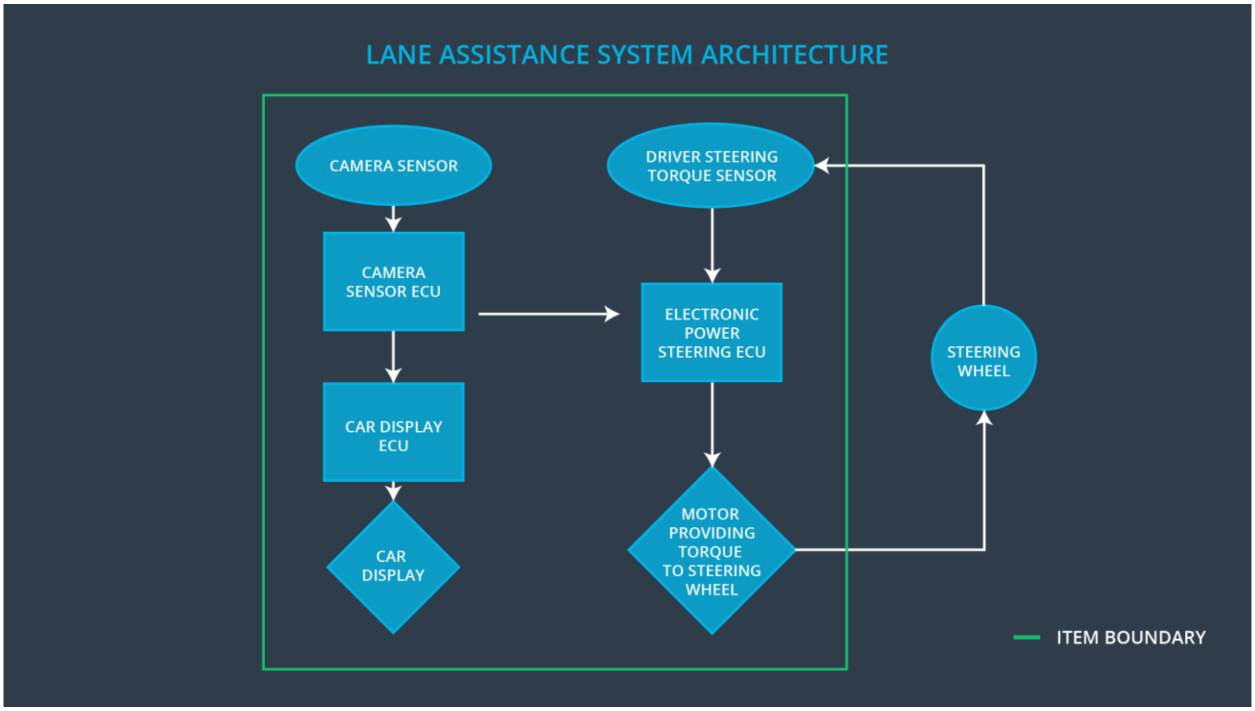
Inputs to the Functional Safety Concept

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 kepping 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 is depicted in the figure below.


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
CAR DISPLAY
MOTOR PROVIDING TORQUE TO STEERING WHEEL
ITEM BOUNDARY

Description of architecture elements

Element	**Description**
Camera Sensor	Physical sensor responsible for detecting lane lines.
Camera Sensor ECU	Electronics hardware and processor responsible for processing camera data, identifying lane markings, determining vehicle position and issuing torque requests to the electronic power steering ECU.
Car Display	Visual indicator responsible for displaying warning to the driver, when the vehicle departs the lane.
Car Display ECU	Electronics hardware responsible for interpreting input from other systems and controlling the car display.
Driver Steering Torque Sensor	Sensor responsible for measuring steering torque input on the steering wheel from the driver.
Electronic Power Steering ECU	Responsible for receiving torque commands from other systems, monitoring the driver torque input and actuating the vehicle steering motor.
Motor	Responsible for applying the 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	LDW function applies MORE oscillating steering torque to the steering wheel.	Driver loses control of the vehicle. Collision with other vehicle or obstacle.

	driver a haptic feedback		
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	LDW function applies oscillating steering torque in the WRONG situation.	Unexpected activation during normal city driving.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	LKA function applies WRONG correction steering torque.	Vehicle is steered off the road, resulting in a crash.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 01-01	LDW oscillating torque amplitude shall be below MAX_TORQUE_AMPLITUDE	C	50ms	Set vibration torque amplitude to 0.
Functional Safety Requirement 01-02	LDW oscillating torque frequency shall be below MAX_TORQUE_FREQUENCY	C	50ms	Set vibration torque amplitude to 0.

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	**Validation Acceptance Criteria and Method**	**Verification Acceptance Criteria and Method**
Functional Safety	Validate MAX_TORQUE_AMPLITUDE	Verify system turns off if MAX_TORQUE_AMPLITUDE is

Requirement 01-01	is high enough to be detected by the driver, while low enough not to cause loss of steering control.	exceeded.
Functional Safety Requirement 01-02	Validate MAX_TORQUE_FREQUENCY is high enough to be detected by the driver, while low enough not to cause loss of steering control.	Verify system turns off if MAX_TORQUE_FREQUENCY is exceeded.

Lane Keeping Assistance (LKA) Requirements:

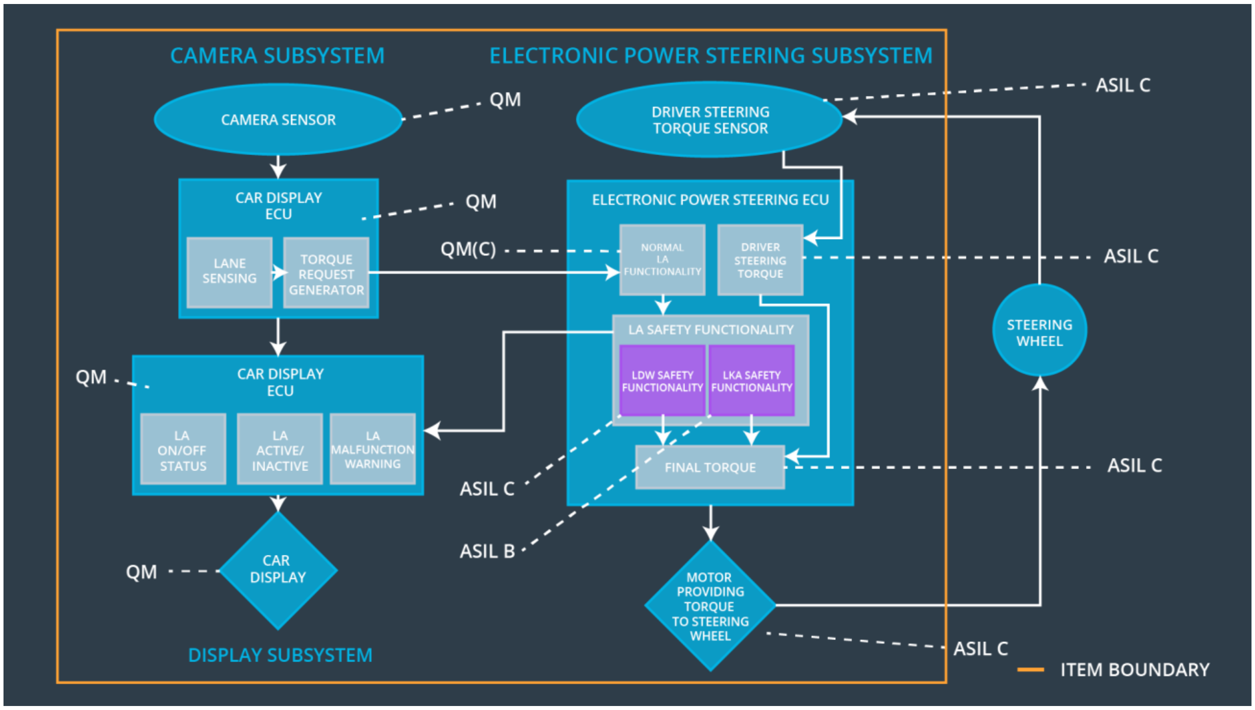
ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is only applied for MAX_DURATION	B	500	Set lane keeping assistance torque to 0

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	Driver testing is used to determine if applying assistance torque for only MAX_DURATION keeps drivers from using the LKA as an autonomous function.	Timing is used to verify that the lane keeping assistance function is turned off after MAX_DURATION.

Refinement of the System Architecture

The refined system architecture is depicted in the figure 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 keeping function shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**Yes**	**No**	**No**
Functional Safety Requirement 01-02	The lane keeping function shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency	**Yes**	**No**	**No**
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that lane keeping assist torque is set to 0 when camera ECU stops detecting lanes.	**Yes**	**No**	**No**

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	turn off the functionality	Malfunction_01/ 02	yes	Car display
WDC-02	turn off the functionality	Malfunction_03	yes	Car display