Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
24-Aug-2018	1.0	Mohamed ZIEDAN	Initial Release

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

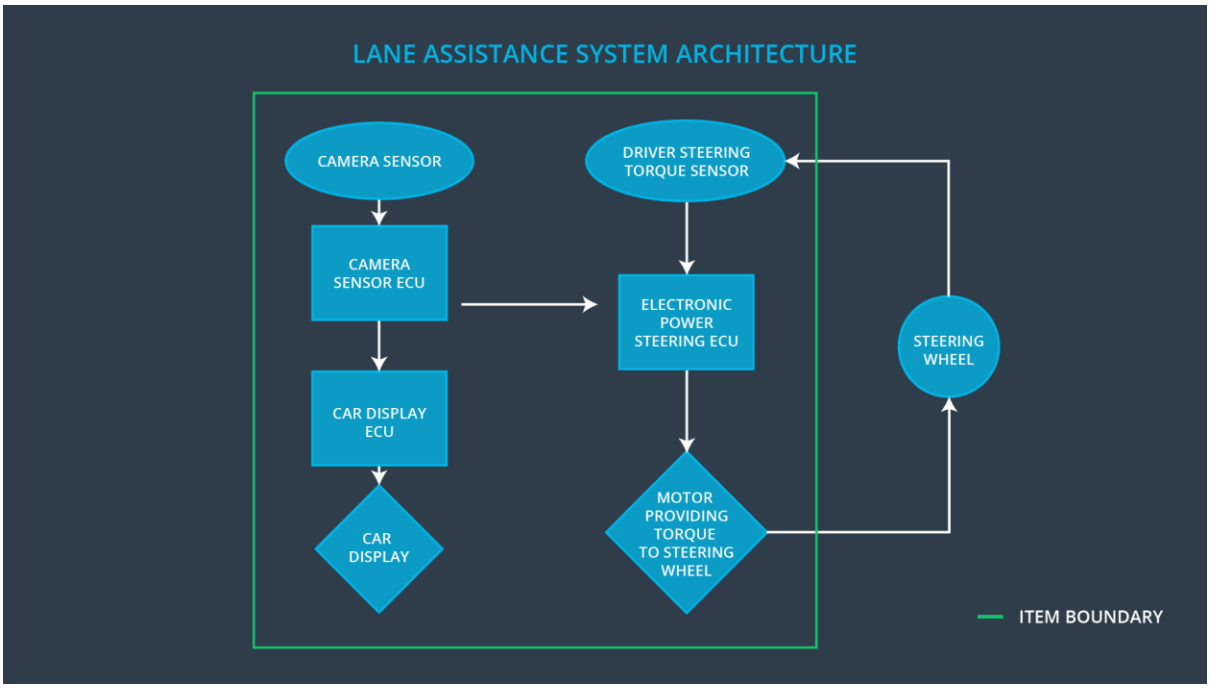
The goal of the Functional Safety Concept is to document the safety goals at a high level. New requirements may be identified to meet these safety goals and allocated to the appropriate part of the system. The document is restricted to the general functionality of the safety goals and does not extend 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 torque from the Lane Departure Warning (LDW) 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 driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Take images of the road
Camera Sensor ECU	detects lane departures, and tells the Electronic Power Steering ECU how hard to turn , and Car Display ECU to display a warning
Car Display	show a warning for the driver
Car Display ECU	receives a warning from Camera ECU, show Warning on Car Display
Driver Steering Torque Sensor	Detect how hard the driver is turning the steering wheel
Electronic Power Steering ECU	Analyze how hard the driver is turning the steering wheel, when it receives a warning from Camera Sensor ECU, it then decides the vibration required to alert the driver, and output a torque value to the motor .
Motor	The motor will provide the torque to 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 lane departure 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 amplitude (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 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	50ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State)	Switch Off Lane Assistance System
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below *Max_Torque_Frequency*	C	50ms (Diagnostic Test Interval + Fault Reaction Time + Time in Safe State)	Switch Off Lane Assistance System

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 how drivers react to different torque amplitudes to prove that we chose an appropriate *Max_Torque_Amplitude* value.	when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	test how drivers react to different torque frequencies to prove that we chose an appropriate *Max_Torque_Amplitude* value.	when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only *Max_Duration*	B	500 ms	Switch Off Lane Assistance System

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 the *Max_Duration* chosen really did dissuade drivers from taking their hands off the wheel.	verify that the system really does turn off if the lane keeping assistance every exceeded *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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below *Max_Torque_Amplitude*	✓		
Functional Safety	The lane keeping item shall ensure that the lane departure	✓		

Requirement 01-02	oscillating torque frequency is below *Max_Torque_Frequency*			
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only *Max_Duration*	✓		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the functionality	Functional Safety Requirement 01-01 is violated	YES	Display Warning on display system, and different Haptic feedback on the steering wheel
WDC-02	turn off the functionality	Functional Safety Requirement 02-01 is violated	YES	Display Warning on display system, and beep sound.