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

23 – May – 2018	1.0	Rajagopala Rao Srinadhuni	Functional Safety Concept – Discussing Safety using a High Level Design perspective

Table of Contents

Purpose of the Functional Safety Concept

Functional Safety Concept refines Safety Goals formulated during the Hazard Analysis and Risk Assessment phase. These high level goals are used to derive functional safety requirements, which are allocated to suitable item (components) in the item architecture, without necessarily describing the technicalities of the same.

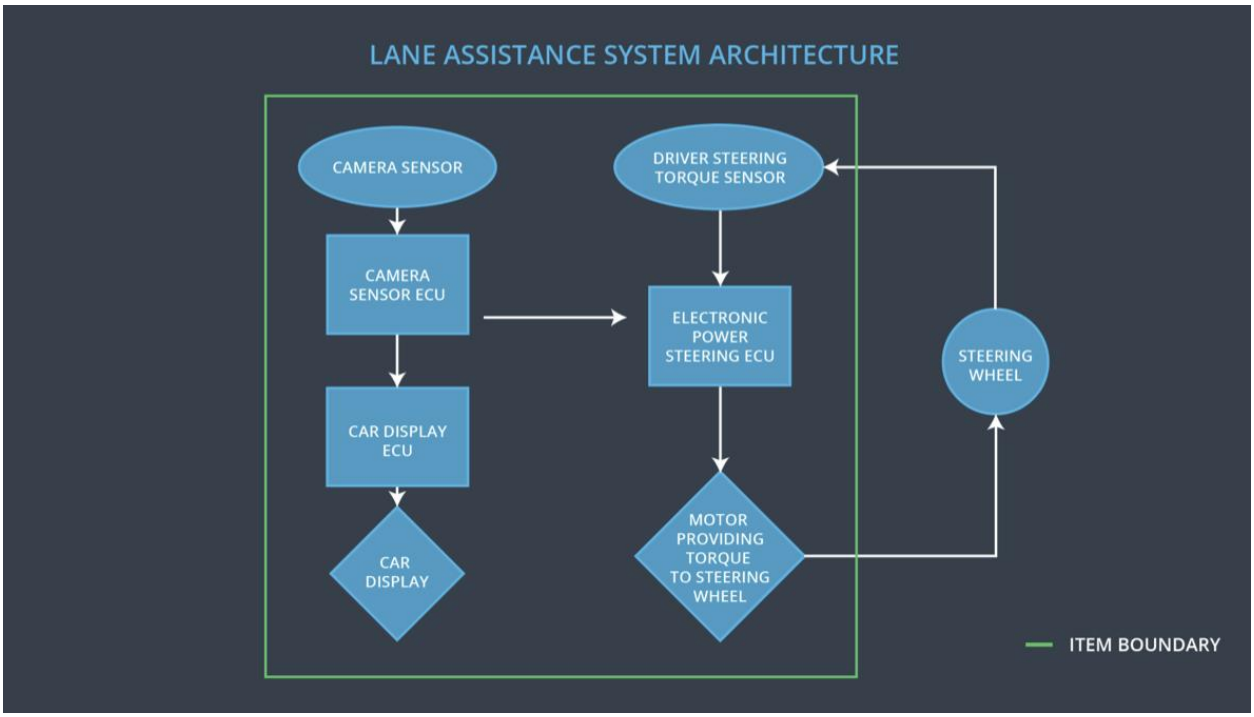
Inputs to the Functional Safety Concept

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 should be limited
Safety_Goal_02	The lane assist feature should function only for a limited duration, after which it stops giving correctional input
Safety_Goal_03	The camera for lane assist system should also account for obstacles in front of the vehicle
Safety_Goal_04	The Lane Assist Feature should compensate for nature of road to optimize the torque introduced

Preliminary Architecture

A preliminary architecture for the lane assistance item that we shall use as base for our requirements



Description of architecture elements

Element	Description
Camera Sensor	Shall be used to monitor lane change activity by the vehicle
Camera Sensor ECU	Is used to incorporate a deep learning model or advanced computer vision techniques such as Hough transform to the data from camera
Car Display	Displays warning messages to the user for unintentional lane changes
Car Display ECU	Monitors the data received from the sensors and issues warning when appropriate
Driver Steering Torque Sensor	Provides a haptic feedback to the user, when warning must be given, through an oscillatory torque
Electronic Power Steering ECU	Takes input from Camera Sensor ECU and guides the motor on the steering to provide correctional torque when an unintentional lane change is detected
Motor	Provides steering assist upon receiving the appropriate feedback

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 frequency (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.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque	WRONG	The lane keeping assistance function may be wrong in sensing an

	when active in order to stay in ego lane		unintentional lane change when sudden obstacles emerge
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	LESS	The lane keeping assistance function generates less torque than needed based on terrain

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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	LDW feature shall turn off (Set Amplitude to zero)
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	LDW feature shall turn off (Set Frequency to zero)

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	Record driver behaviour to various test amplitudes and note the values where driver maintains control	Insert software fault intentionally and see how system handles the malfunction
Functional	Record driver behaviour to various test	Insert software fault intentionally and

Safety Requirement 01-02	frequencies and note the values where driver maintains control	see how system handles the malfunction

Lane Keeping Assistance (LKA) Requirements:

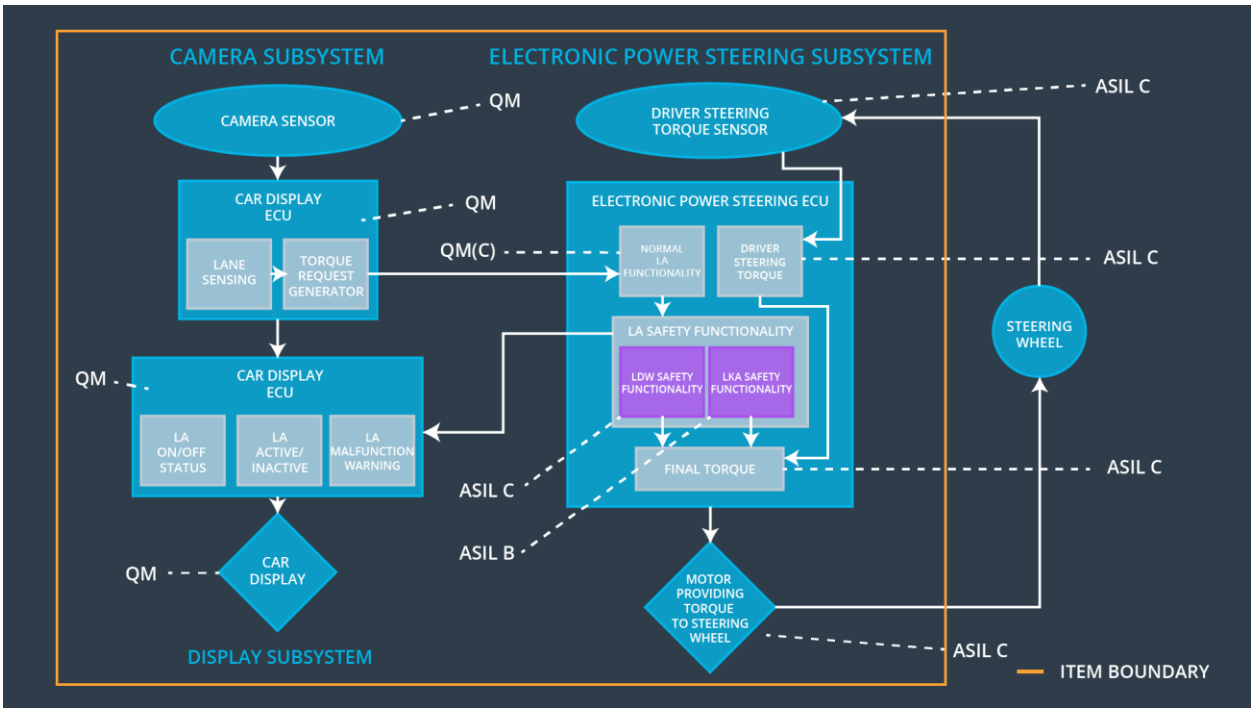
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Lane Keeping Assist switches off
Functional Safety Requirement 02-02	The camera sensor ECU shall monitor obstacles as well, included in the detection model	B	30ms	Lane Keeping system shall turn off
Functional Safety Requirement 02-03	The electronic power steering ECU shall generate steering correction between Min_Correction and Max_Correction value	A	50ms	Lane Keeping Assist switches off

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 with drivers, if the maximum duration actually disuaded them from taking hands off wheel	Run the software and see if it shuts down after given maximum duration
Functional Safety Requirement 02-02	Use situations with obstacles in the testing phase of the learning model of the camera ECU	Test learning model with obstacles in images and see camera sensor ECU output against expected result
Functional Safety	Run vehicle in trial environment	Run vehicle on actual terrains and see how the steering varies for various

Requirement 02-03	simulations with different terrains and compare variation in steering correction given	terrains

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 oscillating torque amplitude is below Max_Torque_Amplitude	**Yes**	**N.A.**	**N.A.**

Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency	**Yes**	**N.A.**	**N.A.**
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	**Yes**	**N.A.**	**N.A.**
Functional Safety Requirement 02-02	The camera sensor ECU shall monitor obstacles as well, included in the detection model	**N.A.**	**Yes**	**N.A.**
Functional Safety Requirement 02-03	The electronic power steering ECU shall generate steering correction between Min_Correction and Max_Correction value	**Yes**	**N.A.**	**N.A.**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Shut down	Malfunction_01 Malfunction_02	Yes	Indicator lamp, indicating maximum torque
WDC-02	Shut down	Malfunction_03	Yes	Indicator lamp blinks twice as system turns off
WDC-03	Shut down	Malfunction_04	Yes	Different shades in indicator lamp, conveying excess or insufficient corrective

				measure
WDC-04	Shut down	Malfunction_05	Yes	Indicator lamp blinks twice as system turns off