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
21.06.2018	1.0	Malgorzata Plonka	Initial version

Table of Contents

Purpose of the Functional Safety Concept

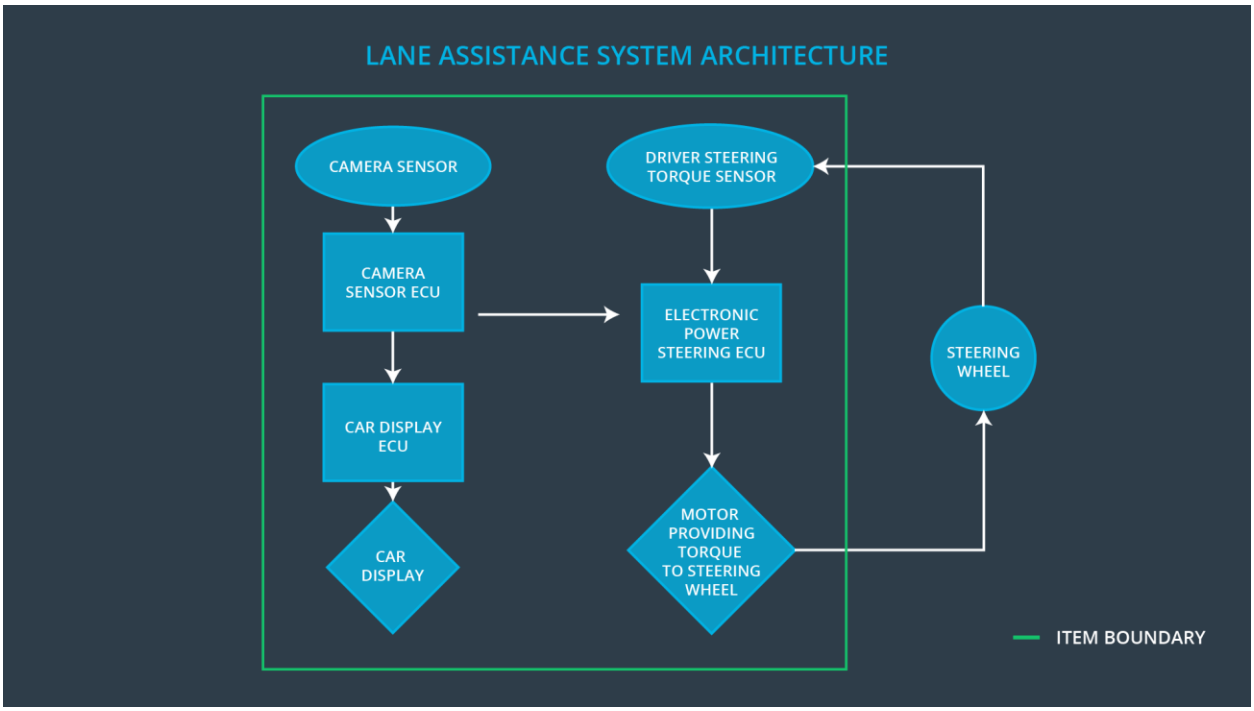
The task of Functional Safety Concept is to document the safety requirements at high level and allocate these requirements to different parts of the item architecture. Technical safety requirements are derived from these safety concepts. The Functional Safety Concept provides instructions how to validate and verify the requirements.

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 limited to particular time interval. The steering torque shall end after a given time interval so the driver does not misuse the system as for autonomous driving.
Safety_Goal_03	The Lane Departure Warning function shall be deactivated as soon as camera sensor stops to work.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated as soon as camera sensor stops to work.

Preliminary Architecture

Following figure describes a preliminary architecture for the lane assistance item.



Description of architecture elements

Element	Description
Camera Sensor	Capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU	Detects lane line location from camera images and generates a torque request to the Electronic Power Steering ECU.
Car Display	Shows warning to driver.
Car Display ECU	Generates visual warning signals triggered by input from Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Use the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning and request

	the necessary torque, which is applied by the motor actuator.
Motor	Applies the torque indicated by the Electronic Power Steering ECU 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 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 it 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	Turn off Lane Departure Warning
Functional Safety Requirement 01-02	The lane-keeping item shall ensure that the lane departure warning torque frequency is below *Max_Torque_Frequency*	C	50 ms	Turn off Lane Departure Warning

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 an appropriate value was chosen - the best one	Verify that system turns off if lane departure warning ever exceeds *Max_Torque_Amplitude*.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that an appropriate value was chosen - the best one	Verify that system turns off if lane departure warning ever exceeds *Max_Torque_Frequency*.

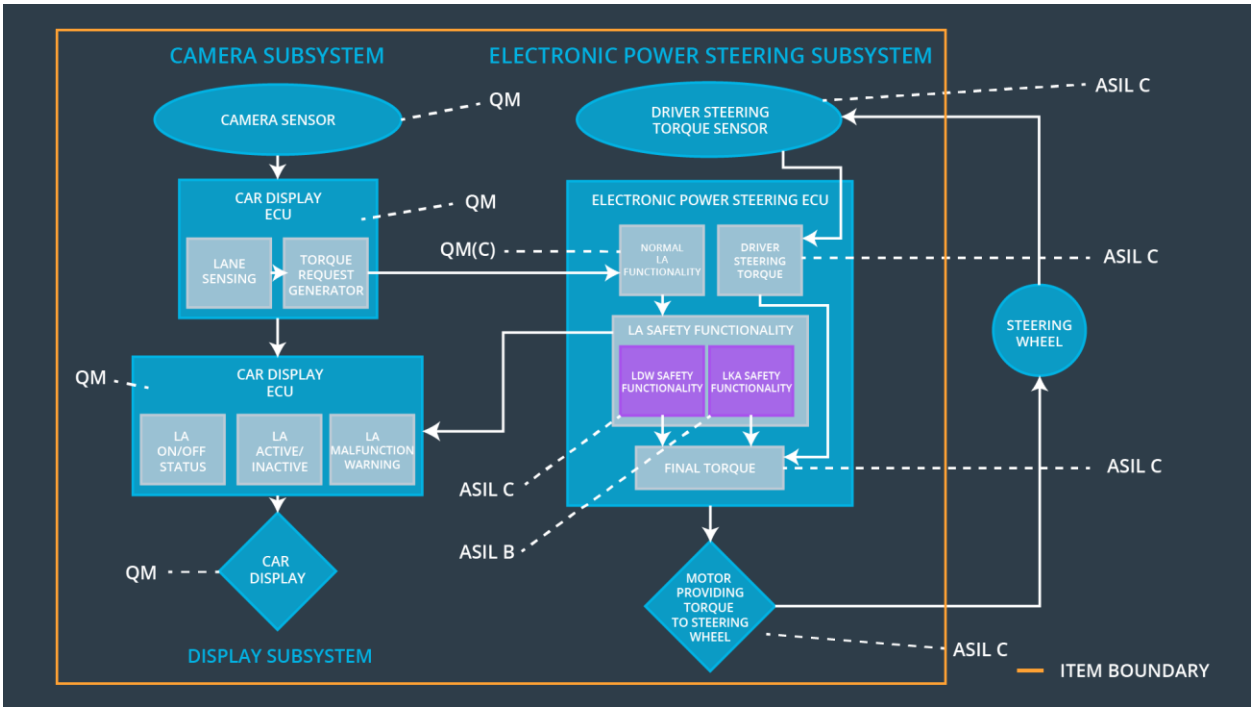
Lane Keeping Assistance (LKA) Requirements:

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	Lane Assistant functionality 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 and validate that the *Max_Duration* chosen really dissuades drivers from taking their hands off the wheel.	Verify that system turns off LKA when torque application 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	The electronic power steering ECU shall ensure that the lane departure oscillating torque	**X**		

01-01	amplitude is below *Max_Torque_Amplitude*			
Functional Safety Requirement 01-02	The electronic power steering ECU 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**		

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked ?**	**Driver Warning**
WDC-01	Turn off LDW functionality	Malfunction_01, Malfunction_02	YES	LDW Malfunction Warning on Car Display
WDC-02	Turn off LKA functionality	Malfunction_03	YES	LKA Malfunction Warning on Car Display