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
28.10.2017	1.0	Simon Ritzel	First Draft and Submission

Table of Contents

Purpose of the Functional Safety Concept

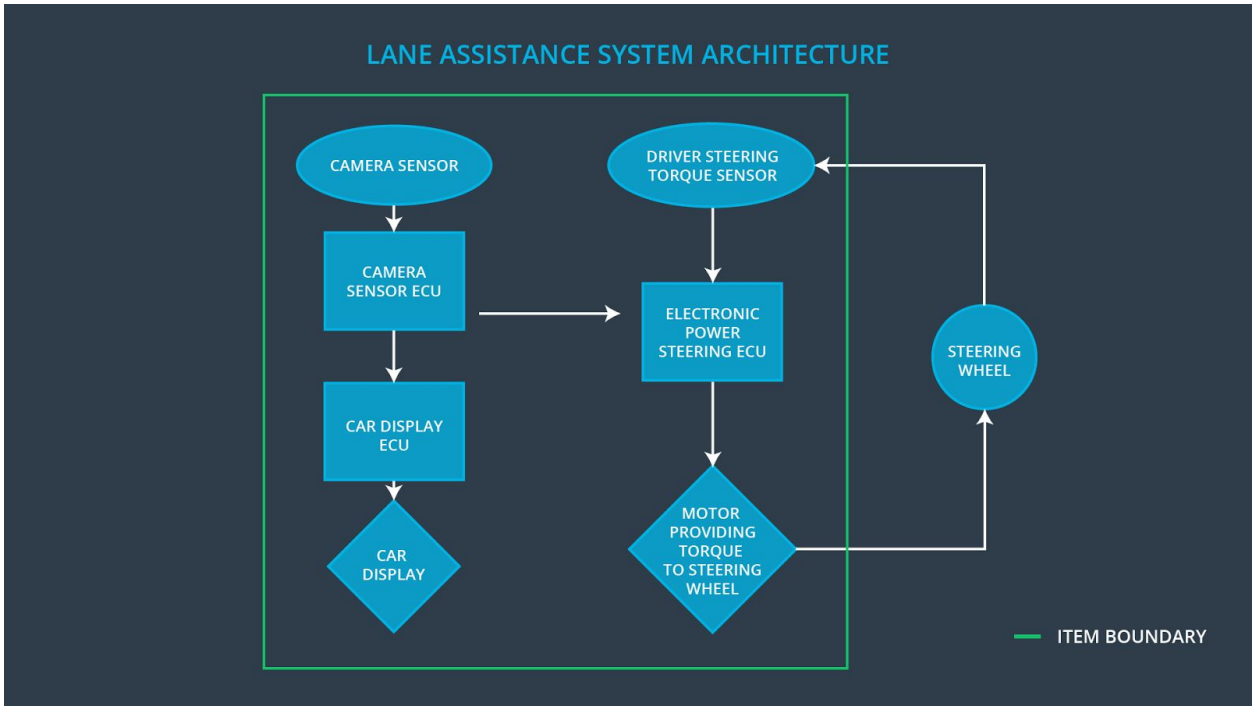
The ultimate goal of the Functional Safety Concept is avoiding accidents by reducing risk to acceptable levels.

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 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.
Safety_Goal_03	The lane departure warning shall be turned off if the Camera Sensor ECU is not able to sense the lane correctly.
Safety_Goal_04	The lane keeping assistance shall be deactivated when driving with low speed.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Capture an image of the road and provide it to the Camera Sensor ECU
Camera Sensor ECU	Lane sensing and generating torque requests
Car Display	LEDs to display signals from Car Display ECU
Car Display ECU	Telling the driver if lane assistance ist on/off or activate/inactive
Driver Steering Torque Sensor	Measures the steering torque from the driver
Electronic Power Steering ECU	Analyze driver steering torque, lane assistance functionality, and final power steering output
Motor	Applies torque from 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration

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	50 ms	LDW function is turned off with visual signal to the driver on the car display
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	50 ms	LDW function is turned off with visual signal to the driver

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 different torque amplitudes with different drivers under different circumstances and determine appropriate value.	Verify that LDW turns off with torque amplitude above threshold and works on amplitudes below threshold.
Functional Safety Requirement 01-02	Test different torque frequencies with different drivers under different circumstances and determine appropriate value.	Verify that LDW turns off when exceeding the threshold and works correctly below set limit.

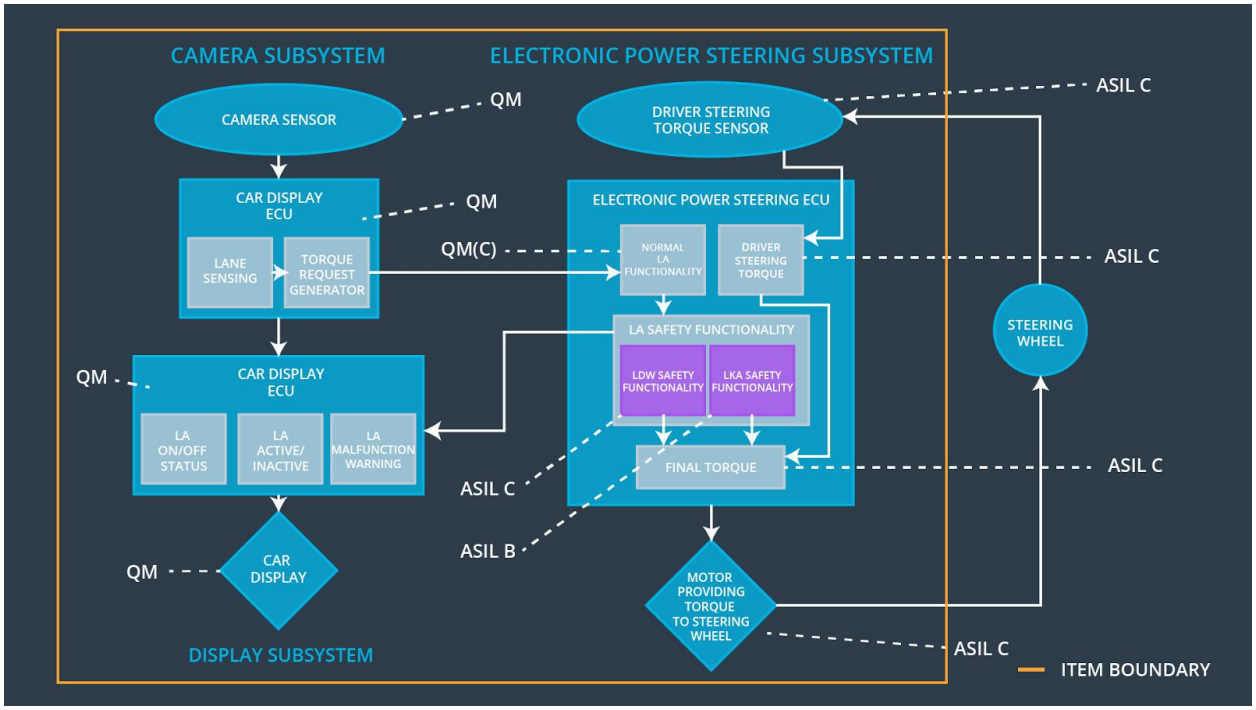
Lane Keeping Assistance (LKA) Requirements:

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 assistance torque is applied for a maximum of Max_Duration	B	500 ms	LKA is turned off with visual signal on the car display to the driver.

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	Validate the Max_Duration interval by testing different values under varying circumstances.	Verify that the LKA turns off after Max_Duration and works while system is used correctly (Driver keeps hands on the steering wheel).

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.	**X**		
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 assistance torque is applied for a maximum of Max_Duration	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW is turned of with visual signal on the car display	Max_Torque_Amplitude or Max_Torque_Frequency is exceeded	YES	YES
WDC-02	LKA is turned off with visual signal on the car display	Max_Duration is exceeded	YES	YES