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
2017-10-17	1.0	Albert Killer	First draft of functional safety concept

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept is a high level approach to look at the general functionality of the item without going into technical detail. The goal is to identify safety requirements and then allocate those requirements to different parts of the item architecture. From the result of the functional safety concept technical safety requirements can be derived within a subsequent technical safety concept. Functional safety requirements also have attributes that are specified in the functional safety concept. Finally to prove that a system actually meets requirements, they have to be verified and validated.

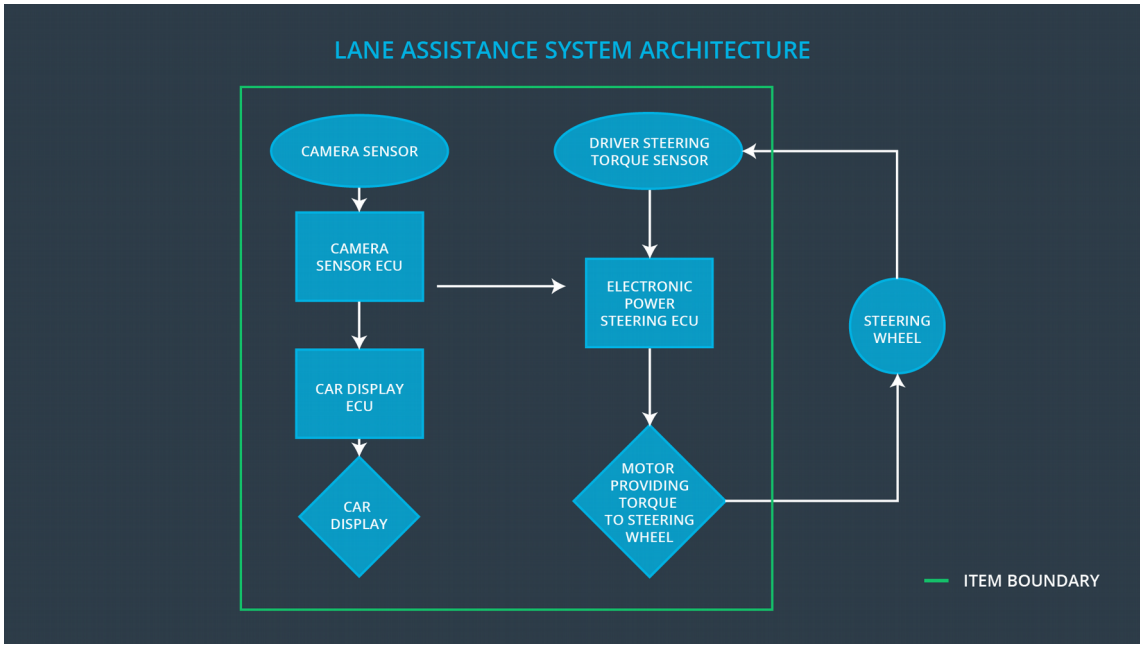
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the LDW function shall be limited.
Safety_Goal_02	LKA function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving.
Safety_Goal_03	LKA function has to be deactivated if camera sensor is not able to detect lanes correctly.
Safety_Goal_04	LKA has to be sensible for different coloring of lane lines, reliably detect and react on merging lanes in advance.

Preliminary Architecture

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



Description of architecture elements

Element	Description
Camera Sensor	Provides camera images to the Camera Sensor ECU.
Camera Sensor ECU	Detects laneline positions from camera images and generates a torque request to the Electronic Power Steering ECU.
Car Display	Shows warning to driver.
Car Display ECU	Generates warning signals triggered by input from Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Delivers steering torque intensity provided by driver to Electronic Power Steering ECU.
Electronic Power Steering ECU	Processes inputs from Camera Sensor ECU, Driver Steering Torque Sensor and computes appropriate Lane Assistance functionality resulting in final torque which is transfered to the steering wheel motor.
Motor	Receives final torque calculated by Electronic Power Steering ECU and applies it 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	Guide-words	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 when active in order to stay in ego lane	NO	Camera sensor is not able to find lane lines due to snow.
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	Camera sensor does not detect yellow lanes of construction site and therefor does not detect lane merging situations correctly. While Keeping the lane LKA introduces lane merging without further precautions.

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	Lane Assistant functionality off
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque *frequency* is below Max_Torque_Frequency	C	50 ms	Lane Assistant functionality off

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.	Verify that system turns off if LKA 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.	Verify that system turns off if LKA ever exceeds Max_Torque_Frequency.

Lane Keeping Assistance (LKA) Requirements:

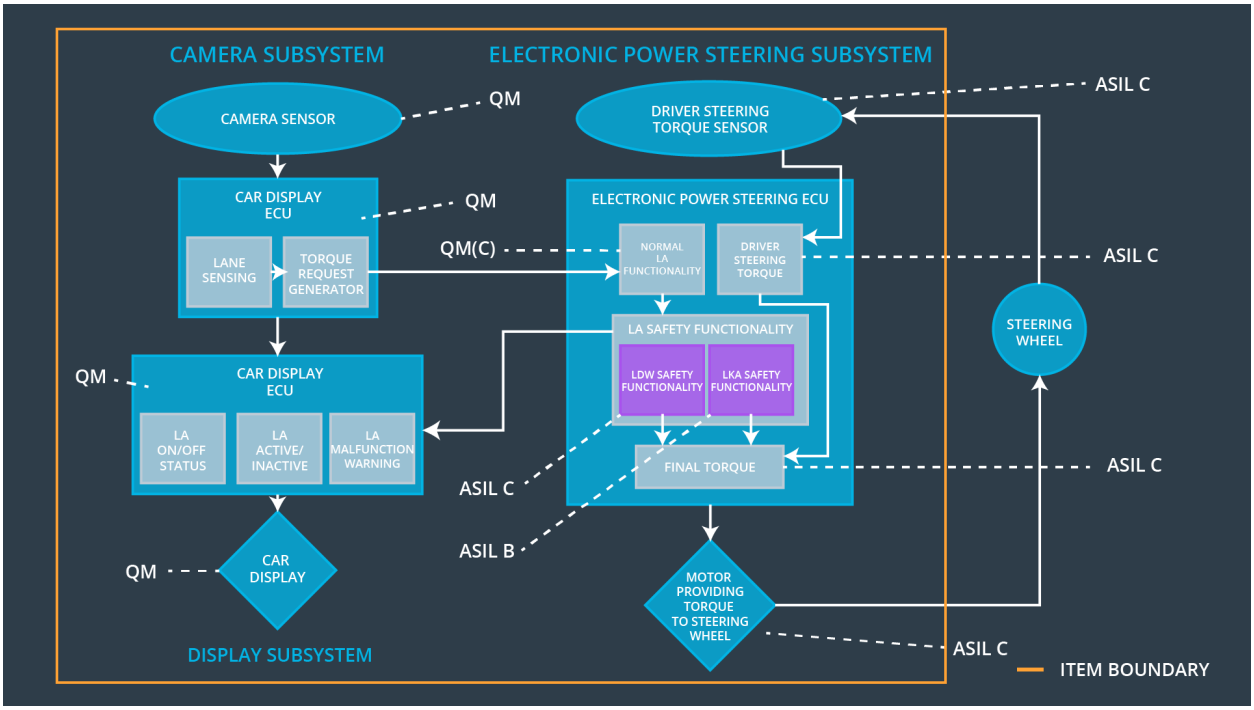
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	Lane Assistant functionality off
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Lane_Not_Found is true	A	50 ms	Lane Assistant functionality off

Functional Safety Requirement 02-03	The camera sensor ECU shall not request torque if Laneline_Is_Yellow is stated true by camera sensor ECU.	D	25 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 if LKA ever exceeds MAX_DURATION.
Functional Safety Requirement 02-02	Test and validate that Lane_Not_Found is stated correctly if lane lines cannot be detected.	Verify that system turns off if Lane_Not_Found is true.
Functional Safety Requirement 02-03	Test and validate that Laneline_Is_Yellow is stated correctly, if lanelines turn yellow.	Verify that system turns off if Laneline_Is_Yellow is true.

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	The electronic power steering ECU shall ensure that the lane	**x**		

Requirement 02-01	keeping assistance torque is applied for only Max_Duration.			
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Lane_Not_Found is true	**x**		
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that lane keeping assistance torque is zero if camera sensor ECU states Laneline_Is_Yellow is true	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Assistant functionality	Malfunction_01	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-02	Turn off Lane Assistant functionality	Malfunction_02	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-03	Turn off Lane Assistant functionality	Malfunction_03	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-04	Turn off Lane Assistant functionality	Malfunction_04	Yes	Lane Assistant Malfunction Warning on Car Display
WDC-05	Turn off Lane Assistant functionality	Malfunction_05	Yes	Lane Assistant Malfunction Warning on Car Display