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
2018-06-04	v0.9	Csathó, Csaba	First draft
2018-06-19	v1.0	Csathó, Csaba	Final version

Table of Contents

Contents

Purpose of the Functional Safety Concept

A functional safety concept produces functional safety requirements from the general functional safety goals. These requirements are allocated to different parts of the item architecture. From the result of the functional safety concept technical safety requirements can be derived in the following step – the technical safety concept. Instructions regarding the validation and verification of the requirements are also provided.

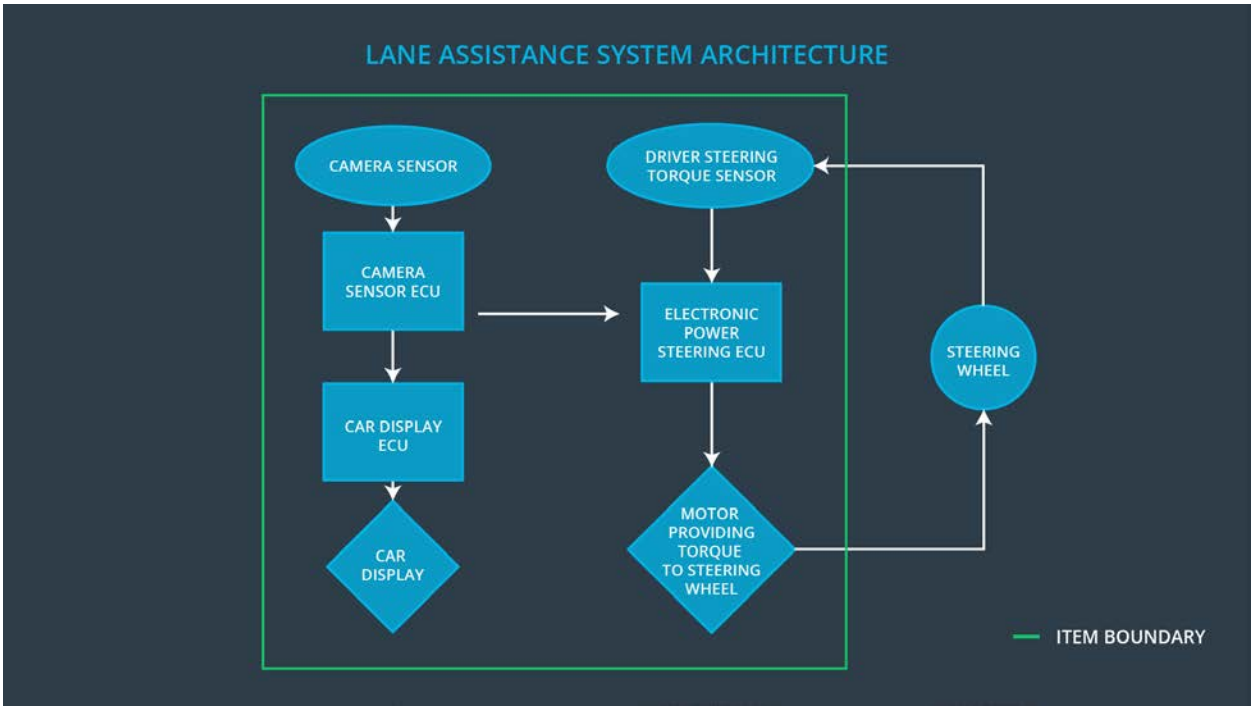
Inputs to the Functional Safety Concept

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 time interval thus the driver cannot use the system for autonomous driving.
Safety_Goal_03	The LKA function has to be deactivated if the camera sensor is unable to detect lanes correctly.
Safety_Goal_04	The LDW function has to be deactivated if the camera sensor is unable to detect lanes correctly.

Preliminary Architecture

The interaction between the three subsystems:



Description of architecture elements

Element	Description
Camera Sensor	Optical sensor for observing lane lines.
Camera Sensor ECU	Processes image data from above and detects lane line positions and issues a torque request to the Electronic Power Steering ECU.
Car Display	Vehicle dashboard that provides feedback of the car's status to the driver (e.g. displaying warnings sings of the LKA/LDW).
Car Display ECU	Handles warning signals that come from the Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Combines the value from above and the torque requested by the by the LKA/LDW and sends the calculated torque value request to the Motor actuator.
Motor	Receives the request from above 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	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting Malfunction
Malfunction_01	The LDW function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE – very high torque amplitude (above limit)	Driver loses control of the vehicle. may result in collision.
Malfunction_02	The LDW function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE – very high torque frequency (above limit)	Driver loses control of the vehicle. may result in collision.
Malfunction_03	The LKA function shall apply the steering torque when active in order to stay in ego lane	NO – no time limitation	LKA is not intended to be used for autonomous driving; may result in collision.
Malfunction_04	The LKA function shall be deactivated when the camera becomes unreliable.	WRONG – unreliable detection	The camera sensor is unable to detect lanes correctly, thus provides incorrect results.
Malfunction_05	The LDW function shall be deactivated when the camera becomes unreliable.	WRONG – unreliable detection	The camera sensor is unable to detect lanes correctly, thus provides incorrect results.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements

F/S ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Intv.	Safe State
Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below `Max_Torque_Amplitude`	C	50 ms	limit torque amplitude
Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below `Max_Torque_Frequency`	C	50 ms	limit torque frequency
Requirement 01-03	If the camera sensor becomes unreliable the LDW system shall be deactivated.	C	25 ms	turn off the complete LDW functionality

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria

F/S ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Requirement 01-01	Testing how drivers handle different torque amplitudes to prove that the right value was selected.	Verifying whether the system limits torque amplitude when an intentionally wrong value was issued.
Requirement 01-02	Testing how drivers handle different torque frequencies to prove that the right value was selected.	Verifying whether the system limits torque frequency when an intentionally wrong value was issued.
Requirement 01-03	Testing various situations when the camera sensor may get occluded.	Verifying whether the system turns off in these scenarios.

Lane Keeping Assistance (LKA) Requirements

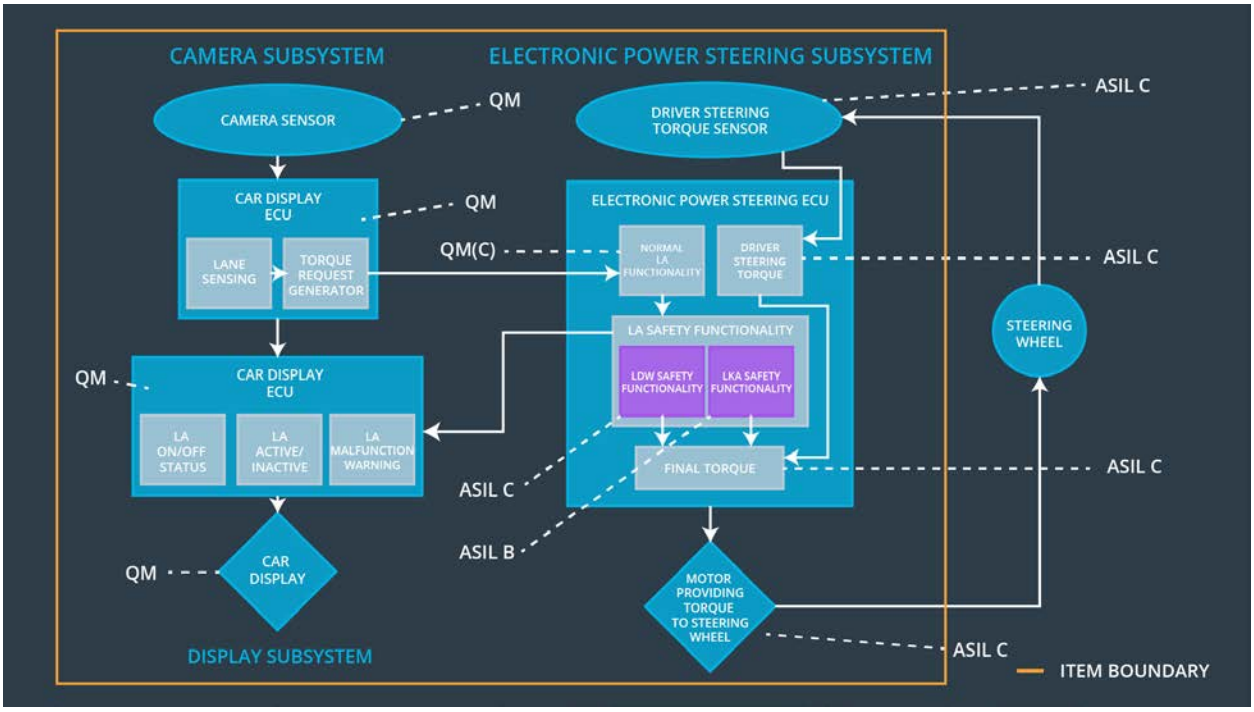
F/S ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Intv.	Safe State
Requirement 02-01	The item shall ensure that the LKA applies the torque for only `Max_Duration` timespan.	B	500 ms	does not apply any torque
Requirement 02-02	If the camera sensor becomes unreliable the LKA system shall be deactivated.	C	25 ms	turn off the complete LKA functionality

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria

F/S ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Requirement 02-01	Testing whether the `Max_Duration` selected really did deter drivers from taking their hands off the steering wheel.	Verifying that the LKA does not apply any torque if the time exceeds `Max_Duration`.
Requirement 02-02	Testing various situations when the camera sensor may get occluded.	Verifying whether the system turns off in these scenarios.

Refinement of the System Architecture

System Diagram after Adding Extra Safety Elements



Allocation of Functional Safety Requirements to Architecture Elements

F/S ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Requirement 01-01	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below `Max_Torque_Amplitude`	X	—	—
Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below `Max_Torque_Frequency`	X	—	—
Requirement 01-03	If the camera sensor becomes unreliable the LDW system shall be deactivated.	X	—	—
Requirement 02-01	The item shall ensure that the LKA applies the torque for only `Max_Duration` timespan.	X	—	—
Requirement 02-02	If the camera sensor becomes unreliable the LKA system shall be deactivated.	X	—	—

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Malfunction_01 Malfunction_02 Malfunction_05	yes	“LDW Malfunction” sign shows on the Car Display
WDC-02	Turn off LKA functionality	Malfunction_03 Malfunction_04	yes	“LKA Malfunction” sign shows on the Car Display