Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
6/25/18	1.0	Pascal Irminger	Functional Safety Concept (init)
6/27/18	1.1	Pascal Irminger	Safe State Refinement

Table of Contents

Purpose of the Functional Safety Concept

The Functional Safety Concept documents the identified system high-level requirements without going into technical details. The goal is to identify safety requirements and then allocate those requirements to relevant parts of the system architecture. From the result of this document, technical safety requirements can be derived within a subsequent Technical Safety Concept.

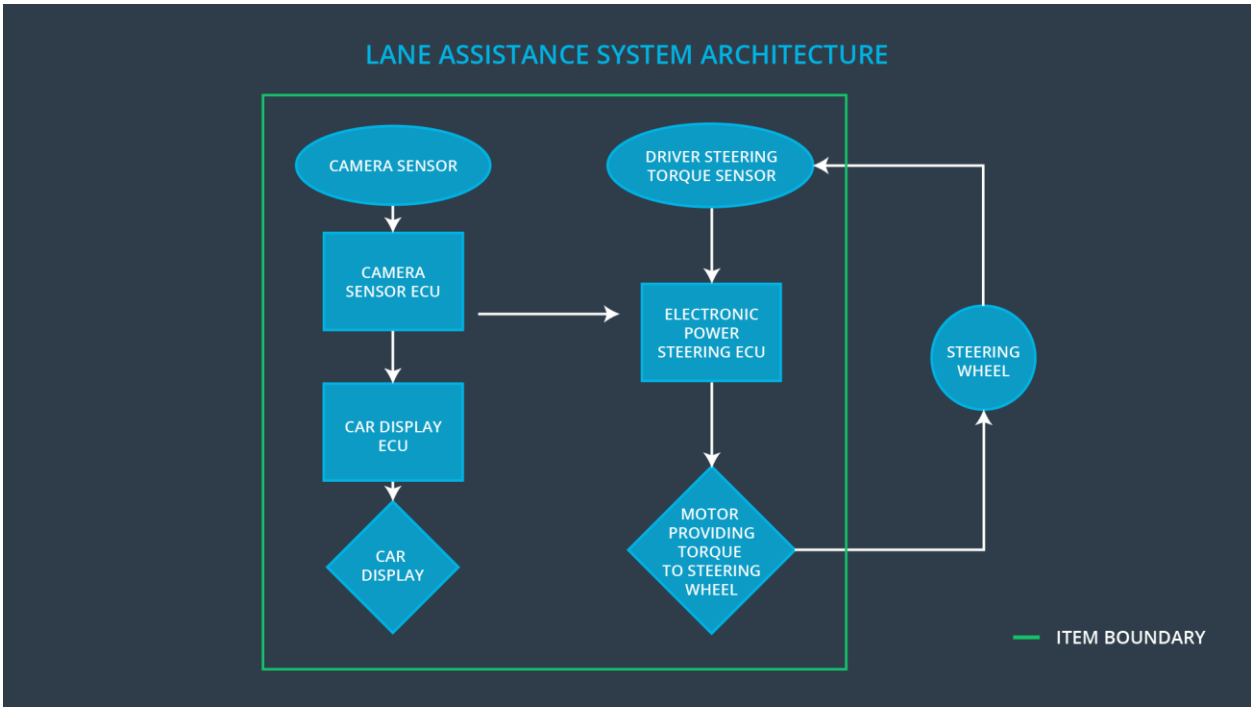
Inputs to the Functional Safety Concept

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	The LKA 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 LDW function shall be deactivated when the camera sensors stop working.
Safety_Goal_04	The LKA function shall always react on time or inform the driver that it has a malfunction and turns itself off.

Preliminary Architecture

The following figure describes the preliminary architecture for the lane assistance item:



Description of architecture elements

Element	Description
Camera Sensor	Captures road images and provides them to the Camera Sensor ECU.
Camera Sensor ECU	Analyzes provided images to calculate the car's position on the road with respect to the road lanes.
Car Display	Provides feedback to the driver by displaying warnings and the LDA function status.
Car Display ECU	Generates warning signals triggered by inputs from the Camera Sensor ECU.
Driver Steering Torque Sensor	Measures the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Uses the information received from the Driver Steering Torque Sensor and the torque requested by the LKA and requests the according torque to be applied by the motor actuator.

Element	Description
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 LDW 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 LDW 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 LKA function is not limited in time duration which leads to misuse as an autonomous driving function.

Malfunction ID	Main Function of the Item Related to Safety Goal Violations	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting Malfunction
Malfunction_04	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	NO	The camera sensor ECU is not able to find lane lines during snowfall (degraded view).
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The camera sensor ECU does not detect yellow lane lines at construction site correctly.

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	Oscillation torque amplitude below Max_Torque_Amplitude.
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	Oscillation torque frequency below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The lane keeping item shall ensure that the lane departure oscillating torque is zero if Lane_Not_Found is stated true by the camera sensor ECU.	B	10 ms	LDW function is turned 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	Validate that Max_Torque_Amplitude is low enough that the driver does not loose control over the car.	Verify that the system turns off whenever the lane departure oscillating torque amplitude exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate that Max_Torque_Frequency is low enough that the driver does not loose control over the car.	Verify that the system turns off whenever the lane departure oscillating torque frequency exceeds Max_Torque_Frequency.
Functional Safety Requirement 01-03	Validate that Lane_Not_Found is stated correctly if lane lines cannot be detected.	Verify that the system turns off whenever Lane_Not_Found is true.

Lane Keeping Assistance (LKA) Requirements:

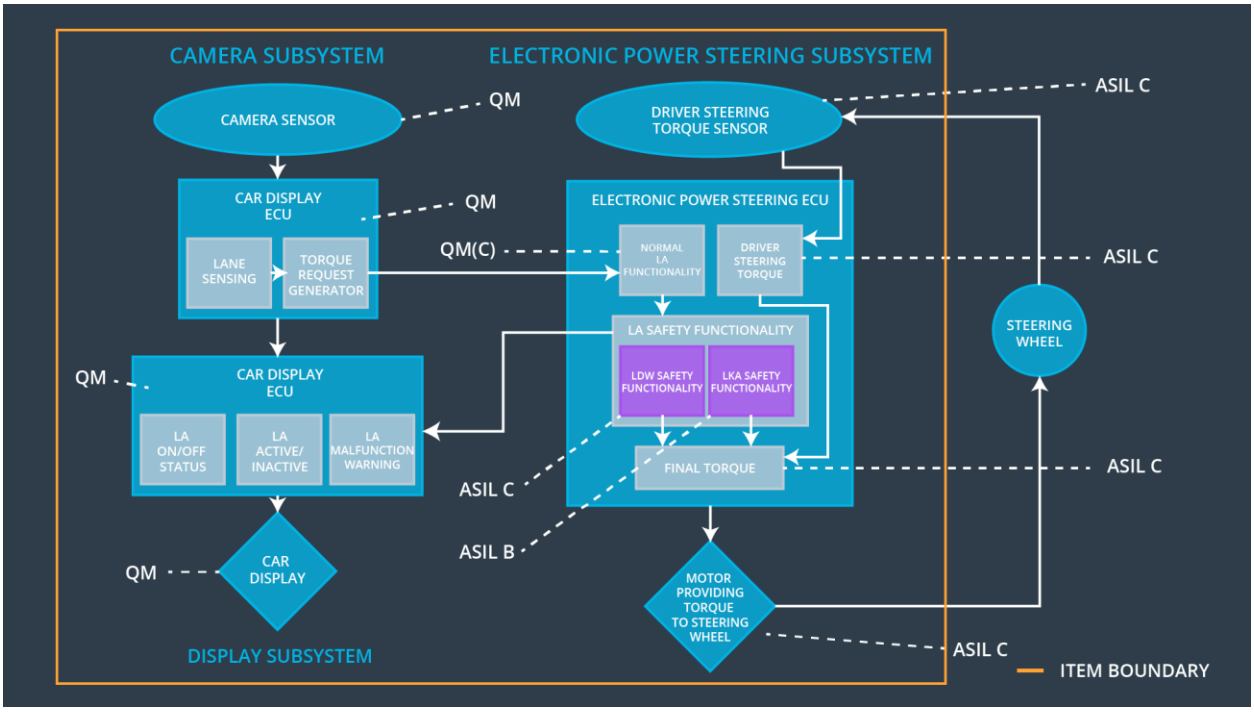
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	LKA torque is zero.
Functional Safety Requirement 02-02	The lane keeping item shall not request torque if Lane_Is_Yellow is stated true by the camera sensor ECU.	A	25 ms	LKA function is turned 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	Validate that Max_Duration really did dissuade drivers from taking their hands off the steering wheel.	Verify that the system turns off whenever the lane keeping assistance exceeds Max_Duration.

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-02	Validate that Lane_Is_Yellow is stated correctly if lane lines turn yellow.	Verify that the system turns off whenever Lane_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 warning oscillating torque amplitude is below Max_Torque_Amplitude.	**x**		

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency.	**x**		
Functional Safety Requirement 01-03	The electronic power steering ECU shall ensure that the lane departure oscillating torque is zero if Lane_Not_Found is stated true by the camera sensor ECU.	**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**		
Functional Safety Requirement 02-02	The electronic power steering ECU shall not request torque if Lane_Is_Yellow is stated true by the camera sensor ECU.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function	Malfunction_01, Malfunction_02, Malfunction_03	Yes	LDW malfunction warning on car display
WDC-02	Turn off LKA function	Malfunction_04, Malfunction_05	Yes	LKA malfunction warning on car display