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
2019-01-23	1.0		First draft

Table of Contents

Table of Contents

Purpose of the Functional Safety Concept

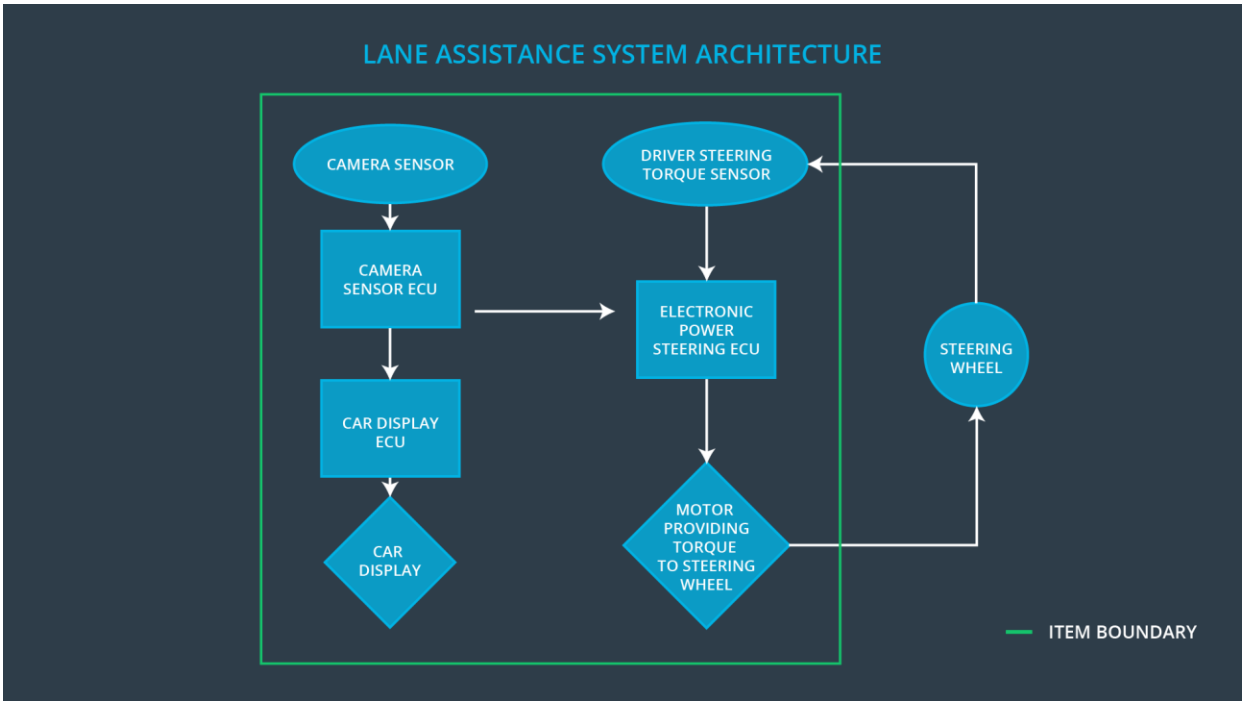
The purpose of the functional safety concept is to identify new functional requirements at a high level and allocate these functional requirements to system diagrams/architecture.

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 keeping assistance function shall be turned off on roads with tight curves so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Records an image of the current road
Camera Sensor ECU	Calculates the position and orientation of the car respectively to the lane lines
Car Display	Displays the status of the functions and the driver warnings
Car Display ECU	Controls the LED for the status and driver warnings
Driver Steering Torque Sensor	Senses the torque the driver applies to the steering wheel
Electronic Power Steering ECU	Controls the torque of the steering wheel motor
Motor	Applies the torque 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	MORE	The lane departure warning function applies an oscillating torque with very high

	torque to provide the driver a haptic feedback		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.

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	50ms	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	50ms	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	The test drivers can still control the car while it is trying to warn the driver, and they also can feel the warning. To validate this, several test drivers will receive different amplitudes and after each test they must document, how they	A testing environment simulates different driver steering torque inputs and measures the amplitude of the LDW. The values measured should not be higher than the limit, with a tolerance of 3%.

	could control the car and if they felt the warning.	
Functional Safety Requirement 01-02	The test drivers can still control the car while it is trying to warn the driver, and they also can feel the warning. To validate this, several test drivers will receive different frequencies and after each test they must document, how they could control the car and if they felt the warning.	A testing environment simulates different driver steering torque inputs and measures the frequency of the LDW. The values measured should not be higher than the limit, with a tolerance of 3%.

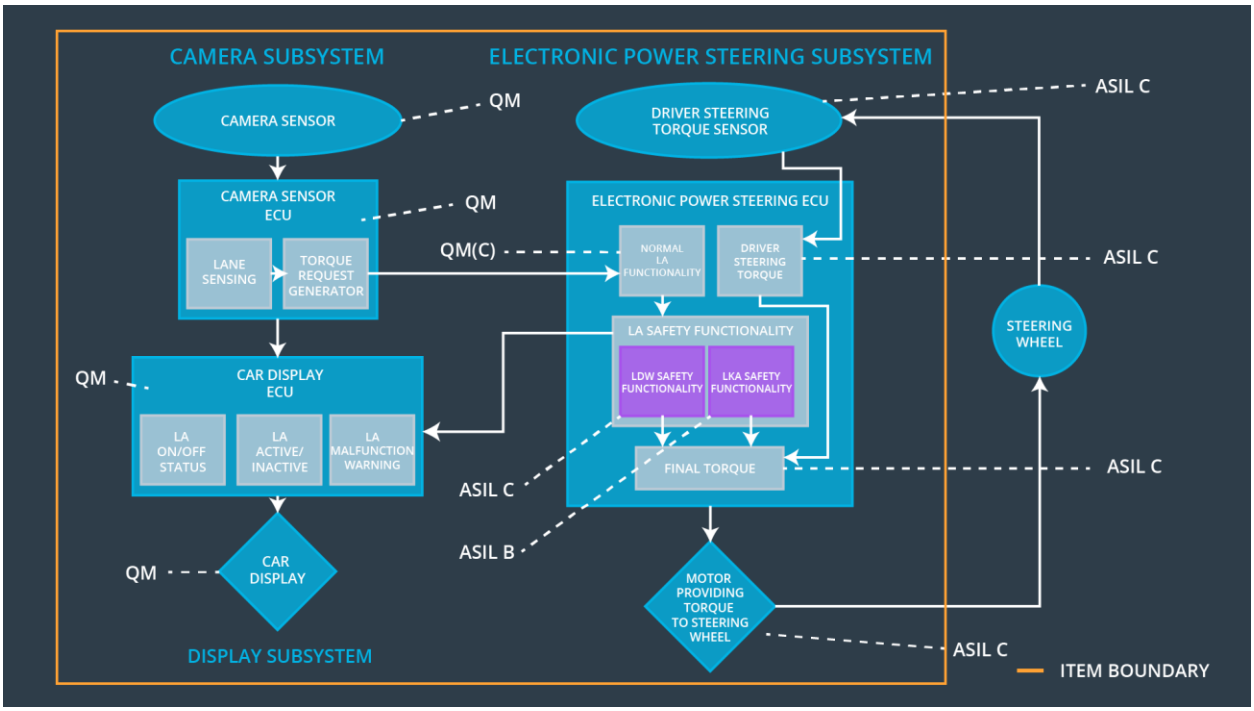
Lane Keeping Assistance (LKA) Requirements:

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	500ms	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	The test drivers do not treat the car as autonomous vehicle, because the LKA function turns off, if the driver does not have his hands on the steering wheel. To validate this, several test drivers will have different duration settings after which the LKA will be disabled and after each test they must document, how likely they would treat the car as autonomous vehicle.	A testing environment simulates steering action of a driver. After some random time, it will stop simulating driver steering torque. The time until the system will be disabled should have Max_Duration with a tolerance of 5%.

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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane keeping item 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**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	OFF	LDW torque or frequency limit exceeded	YES	Display message and turn on a warning light
WDC-02	OFF	LKA driver hands not at steering wheel	YES	Display message and turn on a warning light