Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0
Released on 201-05-22

Document history

Date	Version	Editor	Description
2018-05-22	1.0		Functional safety concept document

Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis
- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept
- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Functional Safety Concept

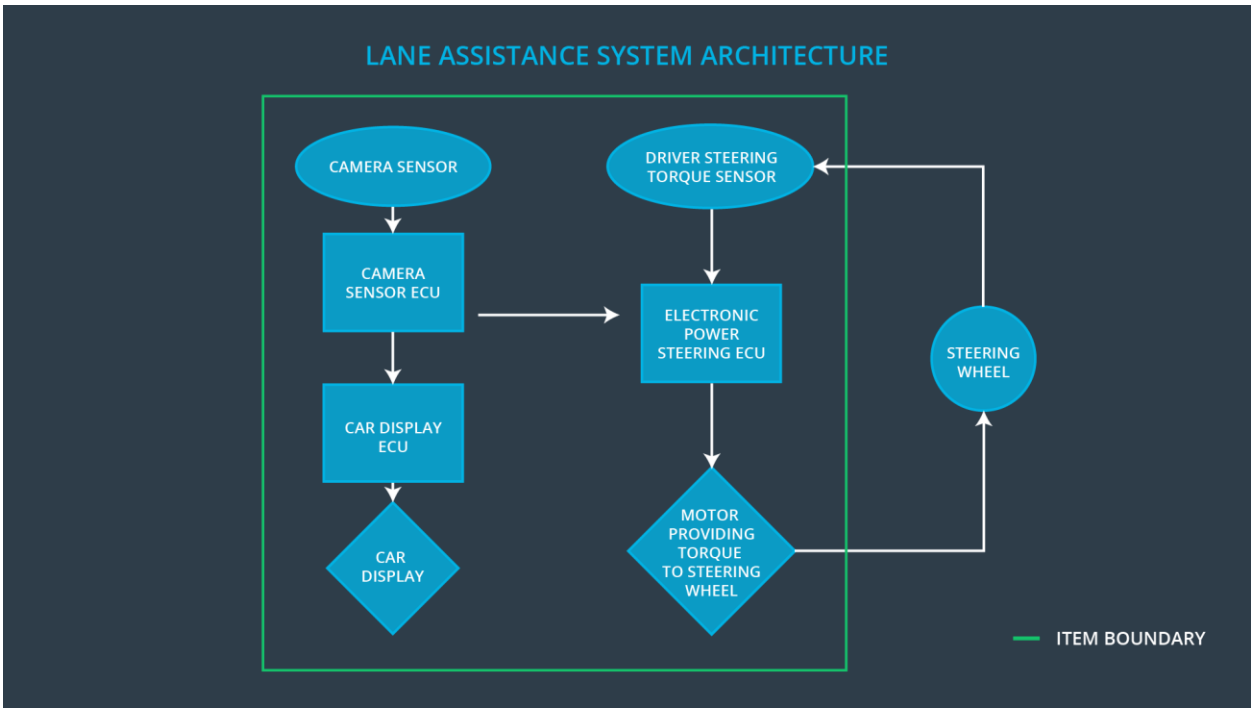
Purpose of functional safety concept document is to identify functional safety requirement and assign those requirements to item's subsystems and elements without getting into technical details.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The lane departure warning system shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.
Safety_Goal_02	The departure warning system shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.
Safety_Goal_03	The lane keeping assistance system shall be time limited.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Sends camera images to camera sensor ECU
Camera Sensor ECU	Identifies lanes and sends torque request to electronic power steering ECU and warning request to car display ECU
Car Display	Shows warning
Car Display ECU	Sends warning signals to car display
Driver Steering Torque Sensor	Monitors steering torque provided by driver and sends it to electronic power steering ECU
Electronic Power Steering ECU	Processes torque request from camera sensor ECU and calculate amount of torque to apply based on input from Driver steering torque sensor and sends it to Motor
Motor	Applies amount of torque received from electronic power steering ECU 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	Lane Departure Warning system shall apply an oscillating steering torque to provide the driver a	MORE	The lane departure warning function applies MORE oscillation torque amplitude then

	haptic feedback		specified limit.
Malfunction_02	Lane Departure Warning system shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The lane departure warning function applies MORE oscillation torque frequency then specified limit.
Malfunction_03	Lane Keeping Assistance system shall apply the steering torque when active in order to stay in ego lane	NO	The Lane Keeping Assistance system has NO time limit which results in misuse as autonomous vehicle.

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 departure warning system shall ensure that oscillation torque amplitude applied to steering wheel is limited.	C	50 ms	Torque amplitude set to 0
Functional Safety Requirement 01-02	The Lane departure warning system shall ensure that oscillation torque frequency applied to steering wheel is limited.	C	50 ms	Torque frequency set to 0

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional	Perform tests on driver’s reaction when	Verify that system sets torque

Safety Requirement 01-01	different torque amplitude is applied and prove that appropriate max value is chosen.	amplitude to 0 when torque amplitude greater than max torque amplitude is requested.
Functional Safety Requirement 01-02	Perform tests on driver's reaction when different torque frequency is applied and prove that appropriate max value is chosen.	Verify that system sets torque frequency to 0 when torque frequency greater than max torque frequency is requested.

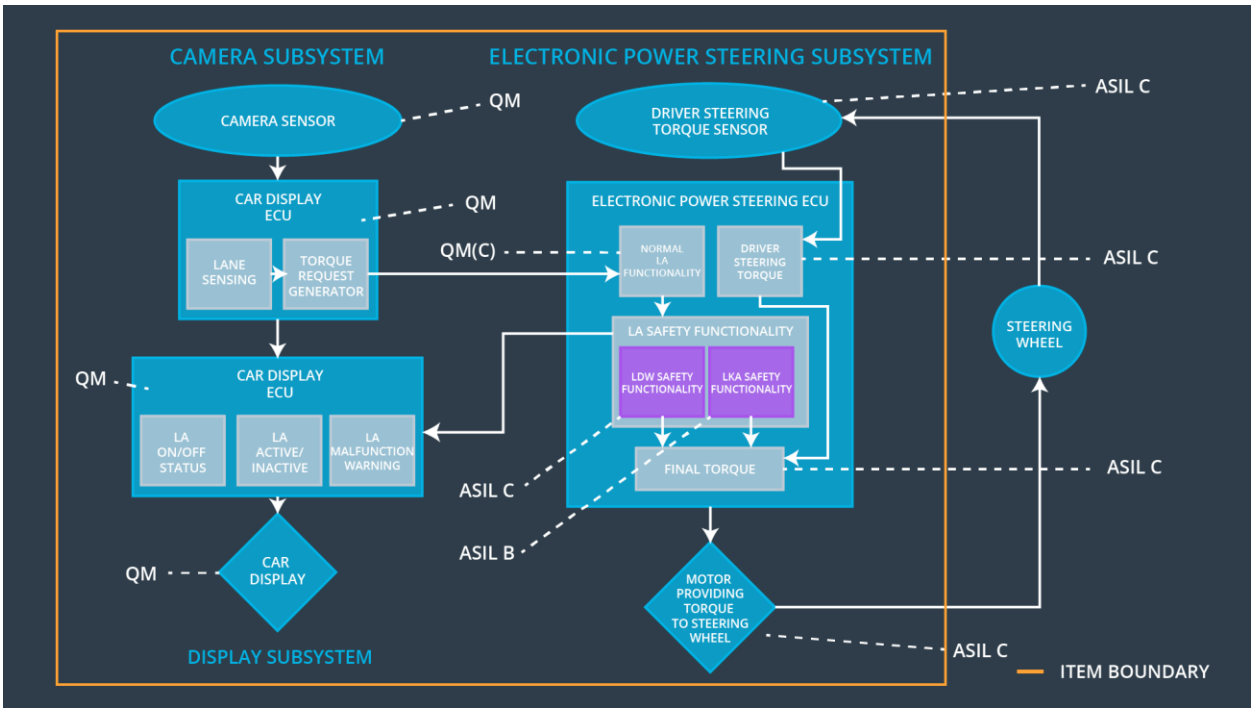
Lane Keeping Assistance (LKA) Requirements:

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	Lane Keeping Assistance system shall apply the steering torque when active in order to stay in ego lane	B	500 ms	Steering torque set to 0

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	Perform tests on time duration chosen to discourage taking off hands from steering wheel and prove that appropriate time duration is chosen.	Verify that system sets steering torque to 0 after time duration.

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 departure warning system shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**x**		
Functional Safety Requirement 01-02	The departure warning system shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**x**		
Functional Safety Requirement 02-01	The lane keeping assistance system shall be time limited.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off lane assistance system	Malfunction_01	YES	Warning on Car display
WDC-02	Turn off lane assistance system	Malfunction_02	YES	Warning on Car display
WDC-03	Turn off lane assistance system	Malfunction_03	YES	Warning on Car display