Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
5/23/2018	1.0	Gireek Bansal	First attempt

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

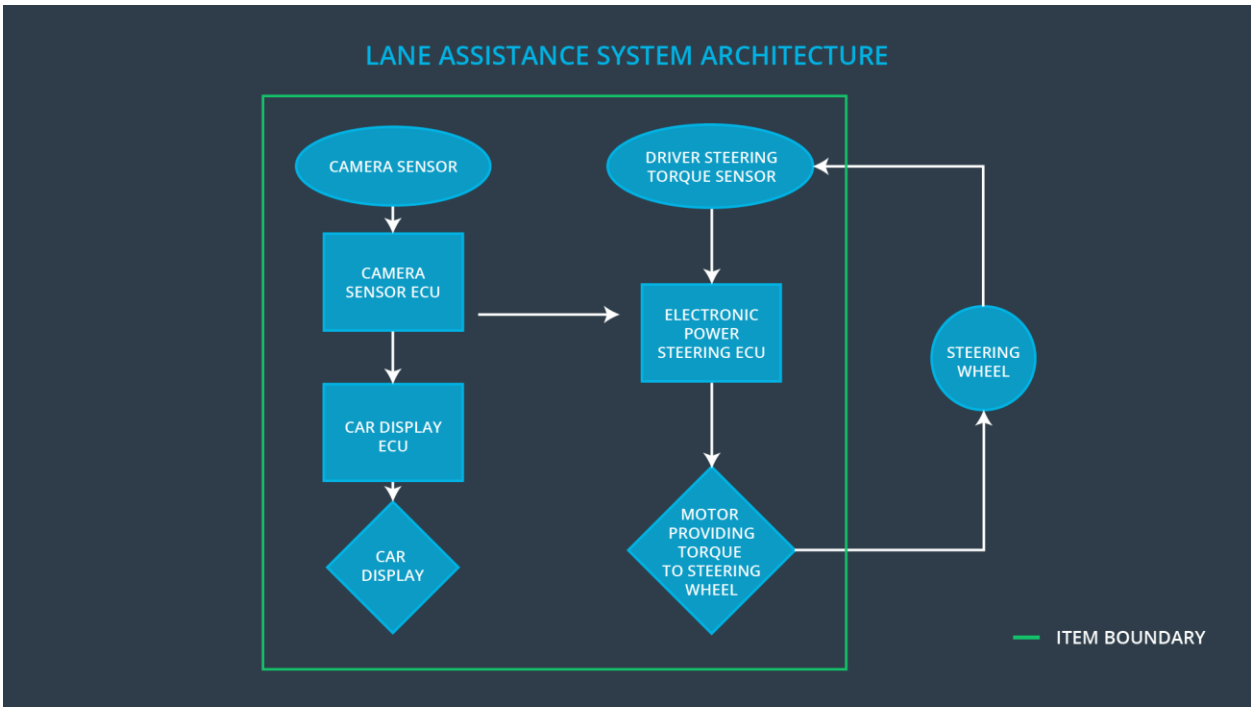
For identifying new requirements and allocating these requirements to system diagrams. The functional safety concept does not go into technical details but only looks at the general functionality of the item. Technical safety requirements will be reached through functional safety concepts.

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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Takes the photos of the external environment and passes them on to the Camera sensor ECU
Camera Sensor ECU	Analyzes the photos to calculate the car's position w.r.t. the lane.
Car Display	A display screen to let the driver know about the car's status and for any type of warnings.
Car Display ECU	The brain behind the Car display to update driver of things to be concerned about.
Driver Steering Torque Sensor	Gives the measure of the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	With the knowledge received from the Driver Steering Torque Sensor it requests the necessary torque to be applied by the Motor actuator.
Motor	Responsible for applying 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 LDW applied an oscillating torque with a very high torque amplitude.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The LDW applied an oscillating torque with a very high torque frequency.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA is not limited in time duration which lead 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.

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 the Max_Torque_Amplitude is the right amount that it doesn't create loss of steering and can warn the driver too.	Verify that the system automatically turns off if the warning exceeds Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate that the Max_Torque_ Frequency is the right amount that it doesn't create loss of steering and can warn the driver too.	Verify that the system automatically turns off if the warning exceeds Max_Torque_Frequency

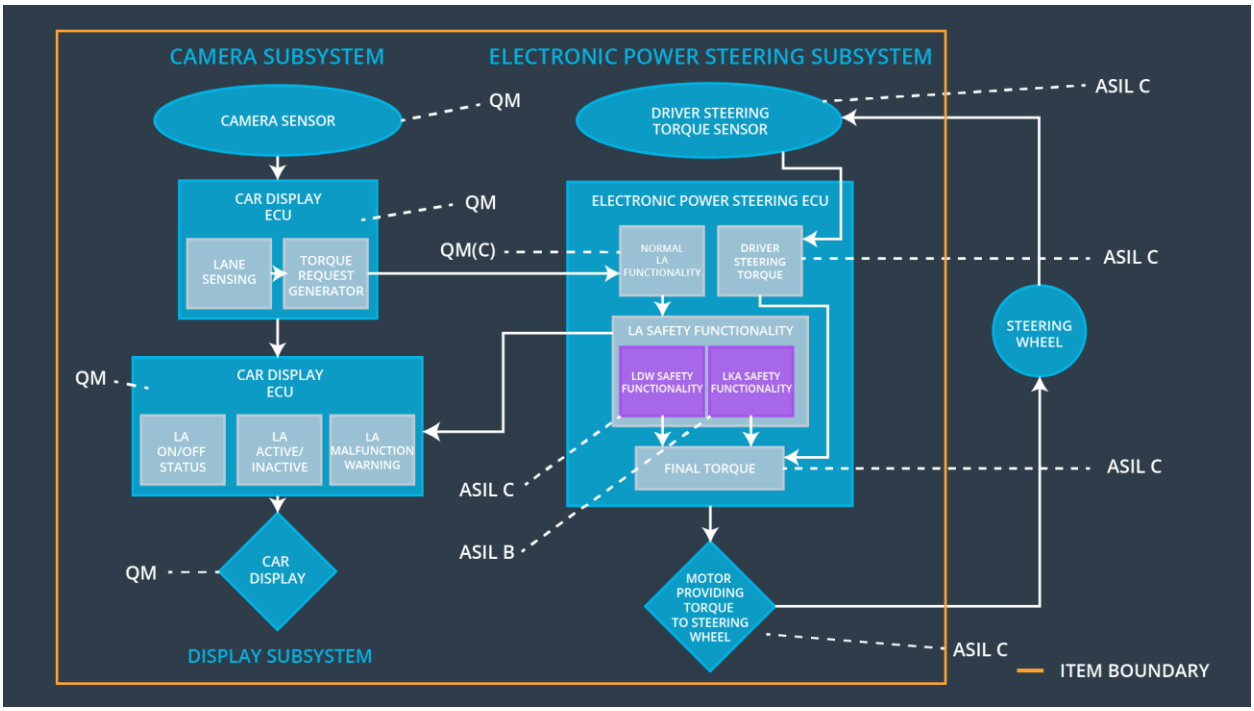
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.	B	500 ms	Lane Keeping Assistance torque is zero

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 the Max_Duration chosen not allow the driver to use the car as self-driving car	Verify the system deactivates automatically if the LKA torque application duration exceeded Max_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 item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**x**		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	**x**		

Functional Safety Requirement 02-01	The Lane Keeping Assistance function shall be time limited, and additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.	**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	Yes	Lane departure warning on car display
WDC-02	Turn off LKA functionality	Malfunction_03	Yes	LKA warning on display