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
2017-10-22	0.1	Wilhelm Nagel	Initial Version

Table of Contents

Purpose of the Functional Safety Concept

The Functional Safety Concept describes the general functionality of the item in terms of high-level performance requirements. Based on the Safety Goals from Hazard Analysis and Risk Assessment, items are identified that need to be adjusted in order to achieve a safe system. The Functional Safety Concept is not concerned with technical details of sub systems – these will be addressed later in the 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 lane departure warning function shall be limited.
Safety_Goal_02	The LKA function shall be time limited and the additional torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.

Preliminary Architecture

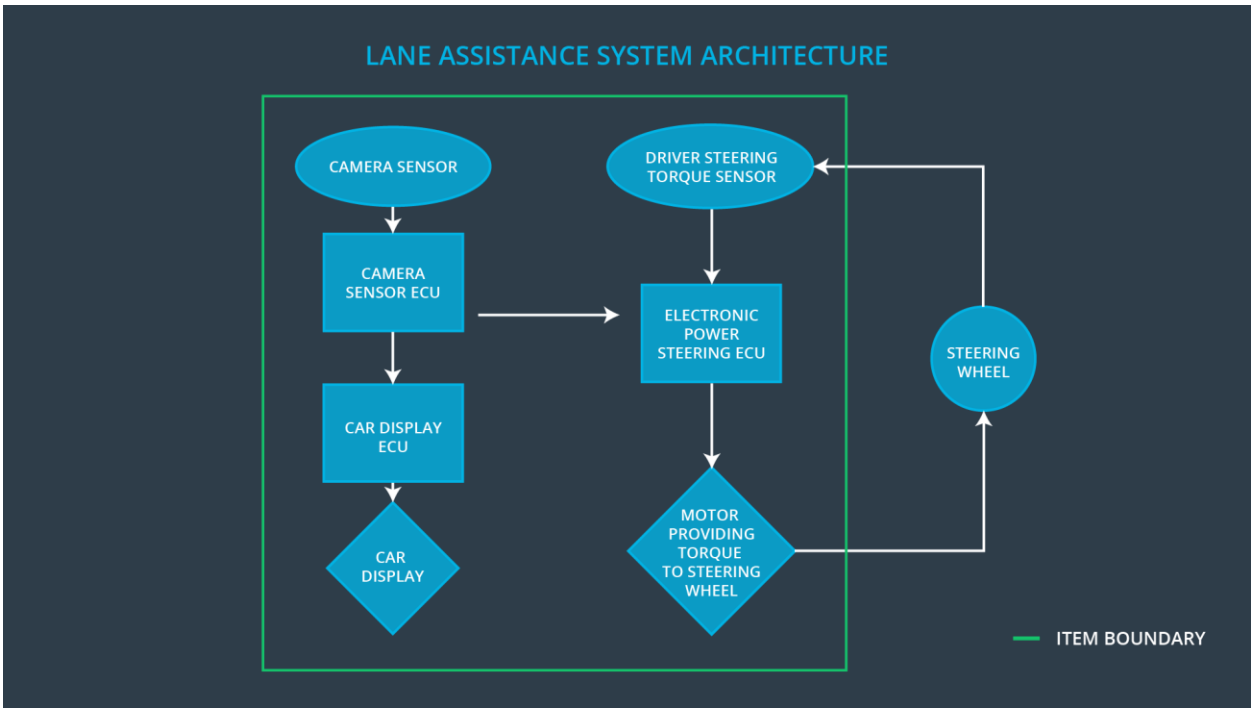

Figure 1: Preliminary System Architecture of the Lane Assistance System

Description of architecture elements

Element	Description
Camera Sensor	Provide images of the road for the Camera Sensor ECU.
Camera Sensor ECU	Process the provided images to detect lane boundaries.
Car Display	Display the current state of the Lane Assistance System, e.g. availability and corrective actions.
Car Display ECU	Process incoming signals from Camera Sensor ECU and control the Car Display.
Driver Steering Torque Sensor	Sense the torque provided by the driver to make sure that driver has not both hands off the steering wheel.
Electronic Power Steering ECU	Process inputs from Driver Steering Torque Sensor and Camera Sensor ECU and control the steering Motor
Motor	Process inputs from Electronic Steering ECU to provide steering torque for 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.

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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	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	Determine a maximum amount of Max_Torque_Amplitude by testing with human drivers. It should be proven that human drivers are comfortable with the chosen value and are able to control the car while steering wheel is vibrating.	When torque amplitude exceeds Max_Torque_Amplitude, LKA system's output is set to zero within the specified 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	Determine a maximum amount of Max_Torque_Frequency by testing with human drivers. It should be proven that human drivers are comfortable with the chosen value and are able to control the car while steering wheel is vibrating.	When torque frequency exceeds Max_Torque_Frequency, LKA system's output is set to zero within the specified 50 ms fault tolerant time interval.

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 LKA torque is applied only for Max_Duration.	B	500 ms	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	By testing with human drivers it should be proven, that the specified deactivation duration of 500 ms is short enough to keep the drivers from taking both hands off the steering wheel.	Verify that electronic power steering ECU provides no more torque after the specified duration of 500 ms.

Refinement of the System Architecture

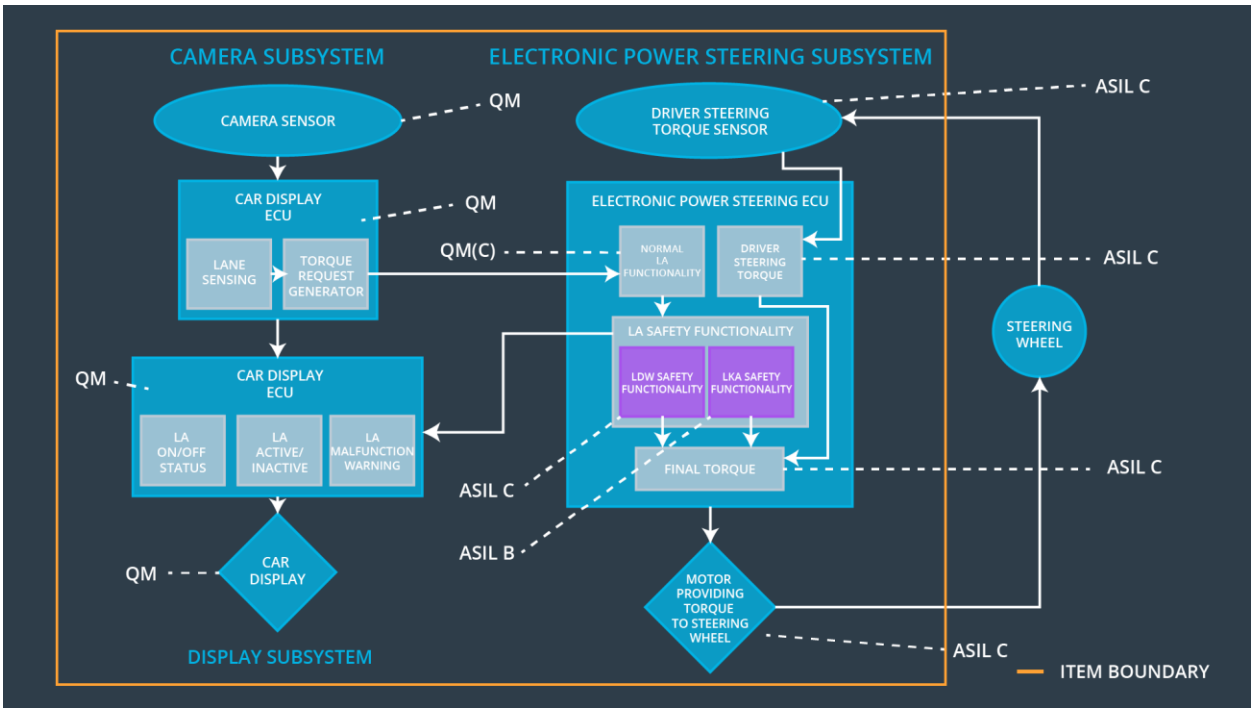

Figure 2: Refined System Architecture of the Lane Assistance System

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 oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The electronic power steering ECU 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 LKA torque is applied only for 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 exceeds defined maximum values for Max_Torque_Amplitude or Max_Torque_Frequency	Yes	Visual warning in Car Display, e.g. by a flashing LED
WDC-02	Off	LKA torque is applied longer than Max_Duration	Yes	Visual warning in Car Display, e.g. by a flashing LED