Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1
2019-03-29

Document history

Date	Version	Editor	Description
2019-03-28	1.0	Sergey Morozov	Completed all document sections
2019-03-29	1.1	Sergey Morozov	Refined functional safety requirements

Table of Contents

Purpose of the Functional Safety Concept

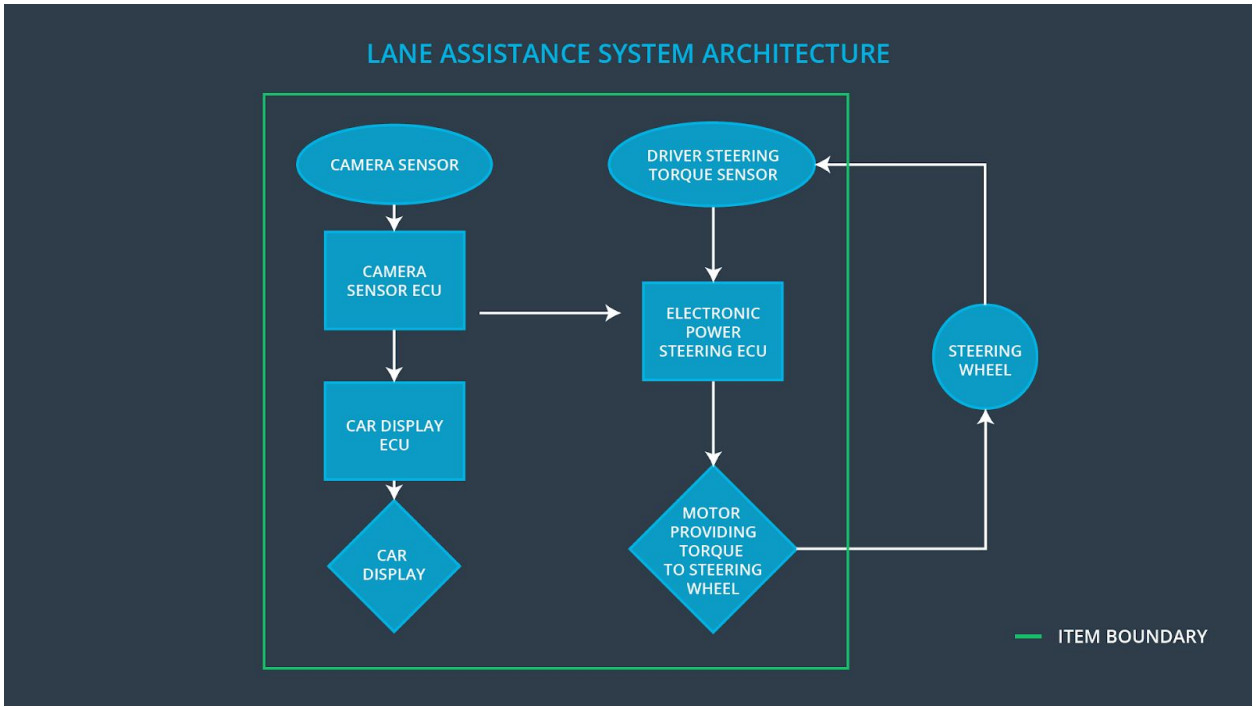
The purpose of the functional safety concept is to refine the safety goals in what are called functional safety requirements and then allocate these safety requirements to the relevant parts of the system diagram. This involves expanding the system architecture with new element blocks, if necessary, and refining the system architecture to handle the new requirements. The functional safety concept does not go into technical details; it looks at the general functionality of the Item.

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.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures images of the road.

Camera Sensor ECU	Identifies when the vehicle has accidentally departed its lane and sends appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Provides the driver with visual notifications about the current state of the lane assistance item.
Car Display ECU	Determines the statuses of lane assistance item subsystems based on the input provided by the Camera Sensor ECU and controls the Car Display to represent this information to the driver in the form of visual notifications.
Driver Steering Torque Sensor	Measures the steering torque applied by the driver to the steering wheel.
Electronic Power Steering ECU	Controls the Motor by determining the actual amount of torque to be applied to the steering wheel based on the input provided by the Camera Sensor ECU and sensory information from the Driver Steering Torque Sensor.
Motor	Applies the torque to the steering wheel as it was determined by the Electronic Power Steering ECU.

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 torque to provide the driver a haptic feedback.	MORE	The lane departure warning 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 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 (Electronic Power Steering ECU) shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 mS	The torque is zero. Warning displayed on the Car Display.
Functional Safety Requirement 01-02	The lane keeping item (Electronic Power Steering ECU) shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 mS	The torque is zero. Warning displayed on the Car Display.

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	Test how drivers react to different torque amplitudes to prove that the Max_Torque_Amplitude is an appropriate value.	When the torque amplitude crosses the limit Max_Torque_Amplitude, the lane assistance output is set to zero within the 50 mS FTTI and the appropriate warning is displayed on the Car Display. Do a software test inserting a fault into the system and seeing what happens.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that the Max_Torque_Frequency is an appropriate value.	When the torque frequency crosses the limit Max_Torque_Frequency, the lane assistance output is set to zero within the 50 mS FTTI and the appropriate warning is displayed on

		the Car Display. Do a software test inserting a fault into the system and seeing what happens.

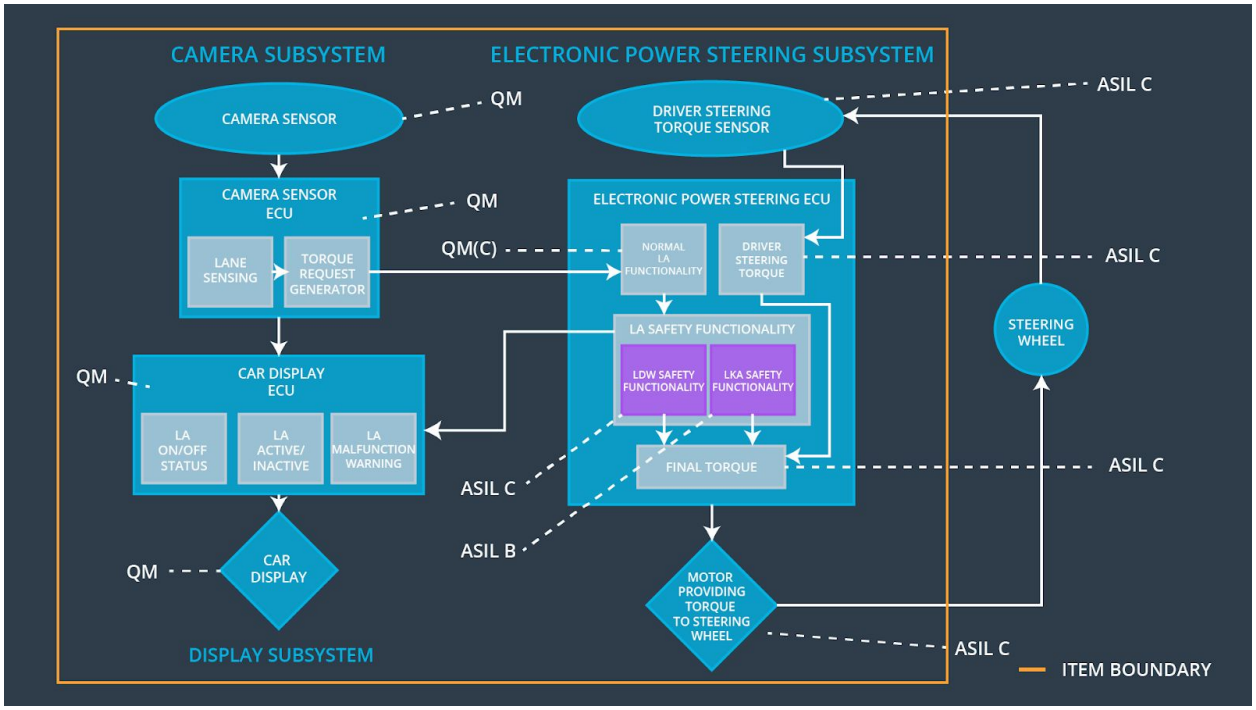
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item (Electronic Power Steering ECU) shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 mS	The torque is zero. Warning displayed on the Car Display.

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	Test how drivers react to different duration values for the lane keeping assistance to prove that Max_Duration is an appropriate value and that it dissuades drivers from taking their hands off the wheel.	Verify that the system really does turn off if the lane keeping assistance when Max_Duration time is exceeded and the appropriate warning is displayed on the Car Display.

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 (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 lane keeping item (Electronic Power Steering ECU) shall ensure that the lane departure oscillating	**X**	-	-

	torque frequency is below Max_Torque_Frequency.			
Functional Safety Requirement 02-01	The lane keeping item (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	Turn off LDW function.	Malfunction_01, Malfunction_02	Yes	Warning displayed on the Car Display
WDC-02	Turn off LKA function.	Malfunction_03	Yes	Warning displayed on the Car Display.