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
23/05/2018	1.0	Sanchit Agrawal	First Submission

Table of Contents

Purpose of the Functional Safety Concept

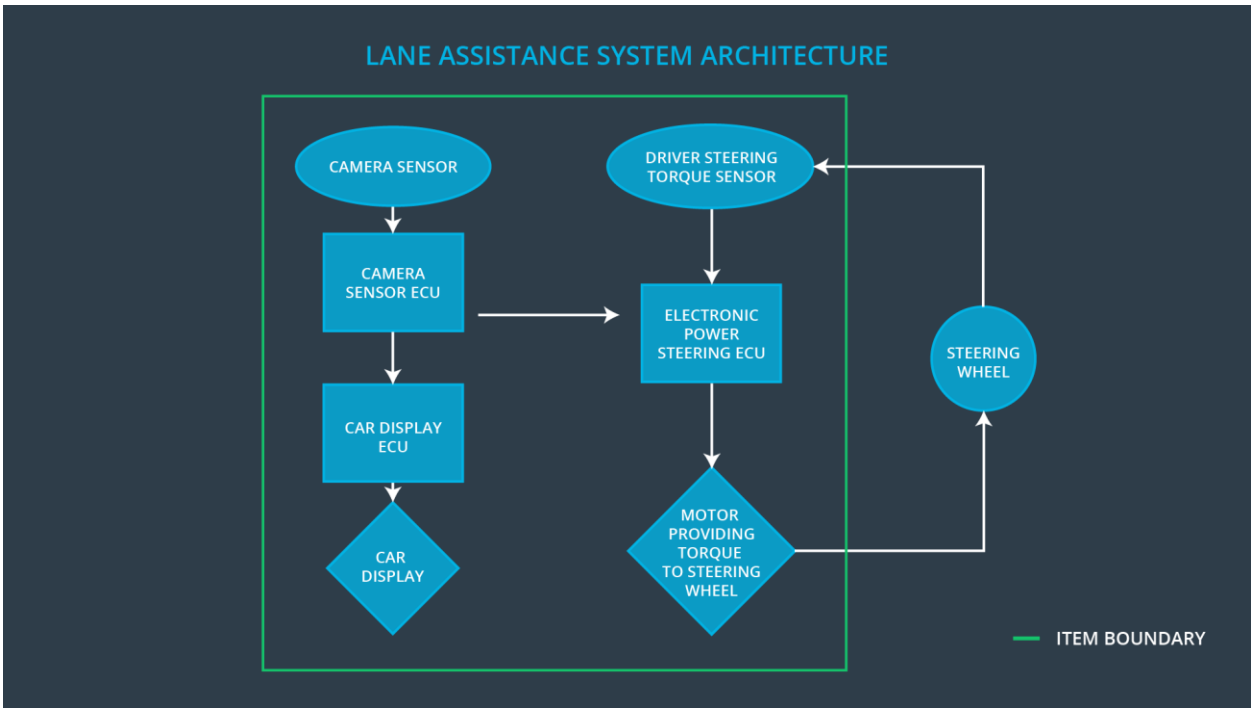
Ultimate goal of functional safety document is to reduce risk to the acceptable level. In this document, system's high level requirements are identified. These requirements are allocated to different part of item architecture. Looking at this architecture design, we need to figure out what subsystem can be used to meet safety goals.

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	Provides images of road to Camera Sensor ECU.
Camera Sensor ECU	Analyze images to get the lane line position and

	generates a torque request to Electronic Power Steering ECU.
Car Display	Shows warning to driver.
Car Display ECU	Generates warning signal triggered by Camera Sensor ECU and Electronic Power Steering ECU.
Driver Steering Torque Sensor	Senses how much torque already been applied by driver.
Electronic Power Steering ECU	Considering the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning. Residual torque is being sent to motor.
Motor	Applies the torque.

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 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 torque amplitude 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	Test driver reaction on different value chosen for torque amplitudes to prove that appropriate value is taken.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety	Test driver reaction on different value	Verify the system does turn off if the Lane Departure Warning exceeded

Requirement 01-02	chosen for torque frequencies to prove that appropriate value is taken.	Max_Torque_Frequency.

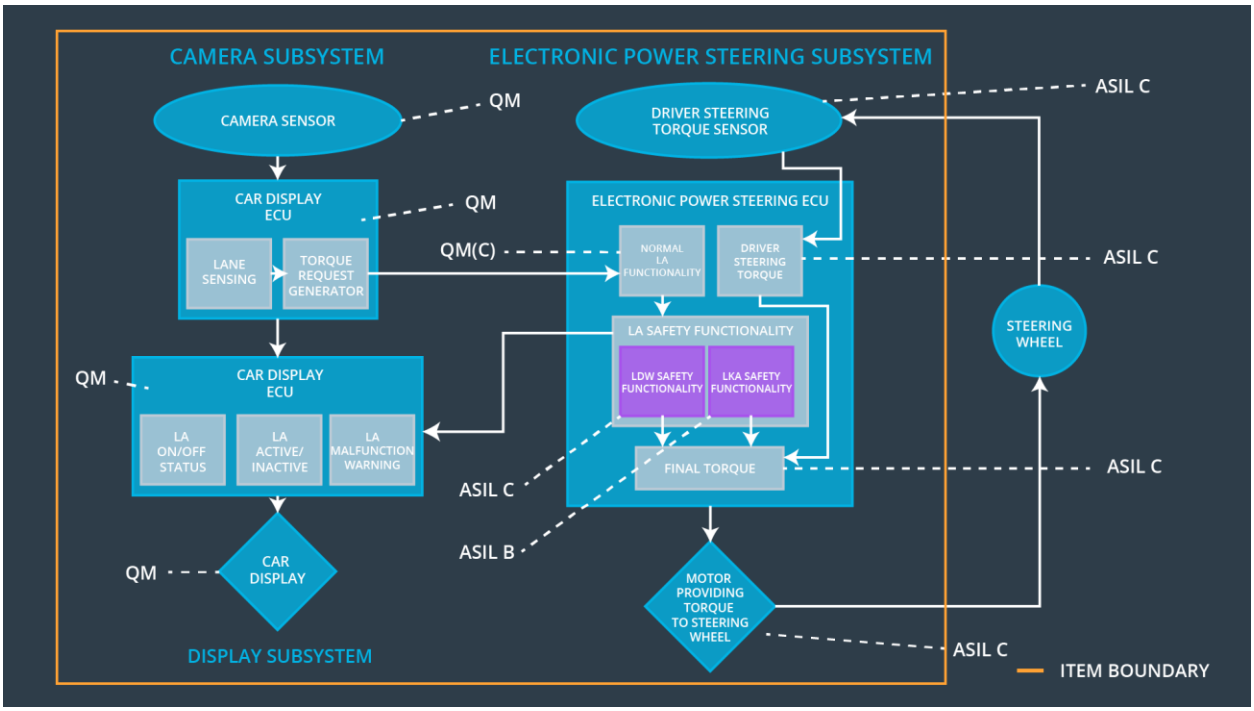
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	B	500 ms	Lane Keeping Assistance system is not activated.

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 driver to use car as self-driving car.	Verify the Lane Keeping Assistance system turn off if application 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.	**YES**	**NO**	**NO**
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	**YES**	**NO**	**NO**
Functional Safety	The electronic power steering ECU shall ensure that the Lane	**YES**	**NO**	**NO**

Requirement 02-01	Keeping Assistance torque is applied only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display