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
10/11/17	1.0	Pedro Lizana	First version of the document.

Table of Contents

Purpose of the Functional Safety Concept

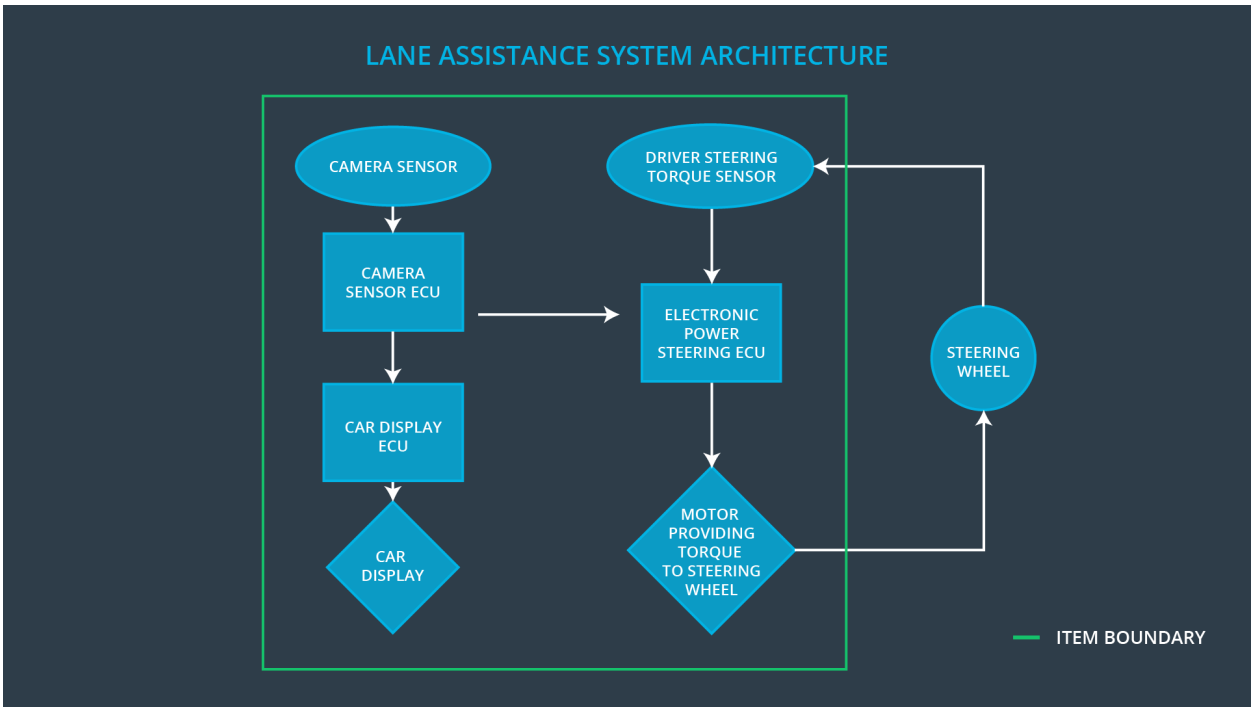
The ultimate goal of functional safety is to avoid accidents by reducing risks to acceptable levels. The functional safety concept translates safety goals into functional safety requirements which are then stored in a document.

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 timer interval so that the driver can not misuse the system for autonomous driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road.
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle has accidentally departed its ego lane, and sends the appropriate messages (torque requests) to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display shows information related to the Lane Assistance item and other items as well.
Car Display ECU	The Car Display ECU controls the lights in the Car Display that tells the driver if the Lane Departure Warning and the Lane Keeping Assistance functions are On/Off or Active/Inactive.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor measures the current torque in the steering wheel, information passed to the Electronic Power Steering ECU.
Electronic Power Steering ECU	The Electronic Power Steering (EPS) ECU will analyze the current driver steering torque and perform checks

	to the torque request generated by the Camera Sensor ECU to output the final torque request that is sent to the Motor.
Motor	The Motor applies the torque request generated by the EPS 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 shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Lane Departure Warning Torque Request shall be set to zero.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	C	50ms	Lane Departure Warning Torque Request shall be set to zero.

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 we chose an appropriate value.	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value.	When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

Lane Keeping Assistance (LKA) Requirements:

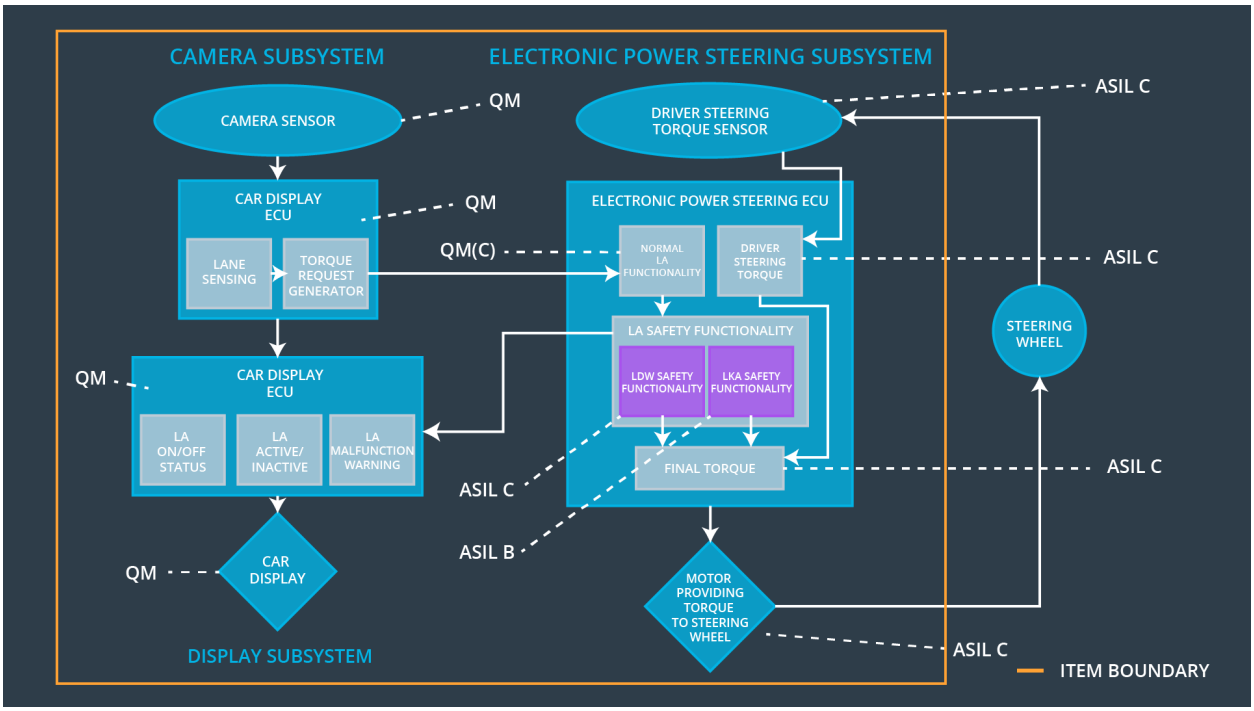
ID	Functional Safety Requirement	AS	Fault Tolerant	Safe State

		IL	Time Interval	
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500ms	LKA Torque Request shall be set to 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	Test and validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel.	We would verify that the system really does turn off in less than 500ms if the lane keeping assistance 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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane keeping assistance torque is	**X**		

02-01	applied for only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW (LA) functionality.	Torque amplitude and frequency exceeds Max_Torque_Ampltiude or Max_Torque_Frequency.	Yes.	Lane Assistance lights in Car Display will turn to Off/Inactive. The LA Malfunction Warning light will also turn on.
WDC-02	Turn off LKA (LA) functionality.	Duration of LKA exceeds Max_Duration.	Yes.	Lane Assistance lights in Car Display will turn to Off/Inactive. The LA Malfunction Warning light will also turn on.