Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0
Released on 2017-11-10

Document history

Date	Version	Editor	Description
November 10, 2017	1.0	Sampayo, Sebastián L.	First submission

Table of Contents

Purpose of the Functional Safety Concept

[Answer what is the purpose of a functional safety concept?]

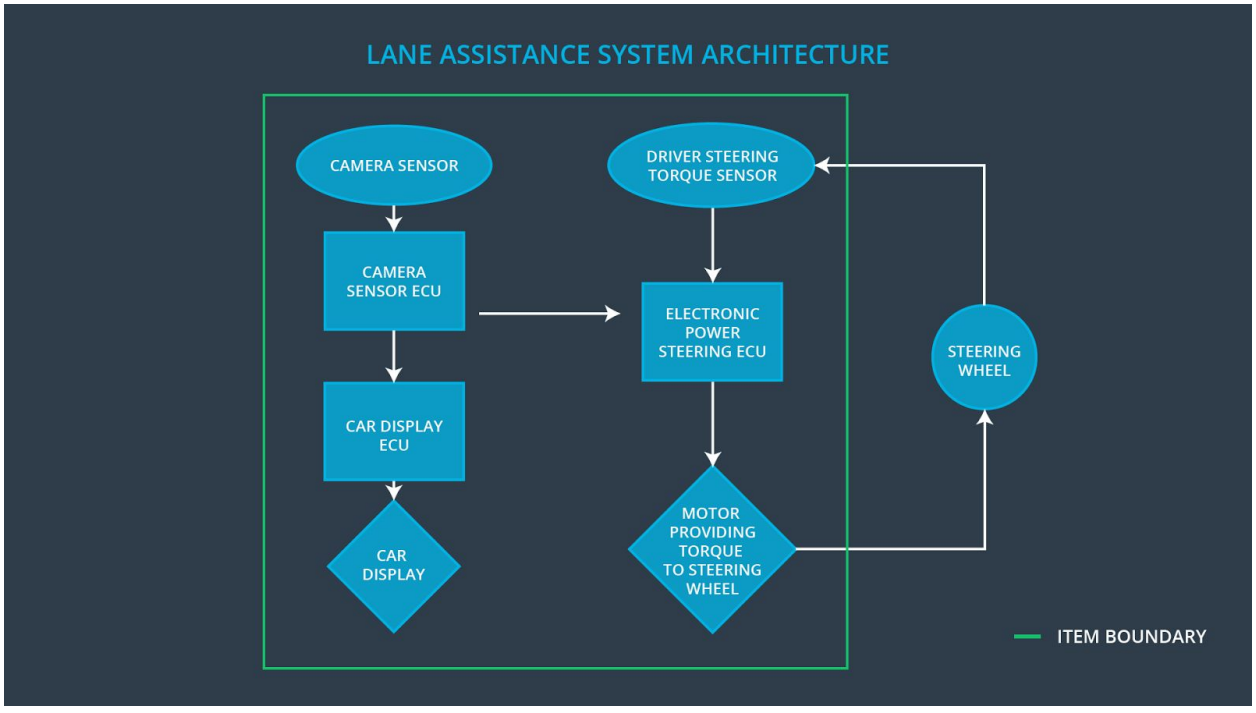
The ultimate goal of functional safety is to avoid accidents by reducing risk to acceptable levels. The purpose of the Functional Safety Concept document is to figure out what subsystems in the system architectural design actually contain high levels of risk and what's needed to prevent accidents. Functional safety requirements are defined and allocated to its appropriate place in the item architecture.

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 LDW function shall be limited.
Safety_Goal_02	The LKA function shall be time limited and the additional steering torque shall end after a given time interval so that the driver is not able to misuse the system as an autonomous driving feature.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Provides raw images of the road and the environment ahead of the vehicle
Camera Sensor ECU	Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake and sends the appropriate message to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Displays warning/alert messages and whether the subsystems are on/off
Car Display ECU	Receives signals from the camera ECU and the different subsystems to show information on the screen.
Driver Steering Torque Sensor	Responsible for measuring the torque provided to the steering wheel
Electronic Power Steering ECU	Responsible for adding the appropriate amount of torque based on a lane assistance system torque request.
Motor	The physical element that actually applies 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

[Instructions: Fill in the functional safety analysis table below.]

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 Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW off
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW 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	For whatever value we end up choosing for the max torque amplitude, we need to validate that we chose a reasonable value. We would need to test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Verify that when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.

Functional Safety Requirement 01-02	For whatever value we end up choosing for the max torque frequency, we need to validate that we chose a reasonable value. We would need to test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Verify that when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval. For this specific case, we would probably do a software test inserting a fault into the system and seeing what happens.

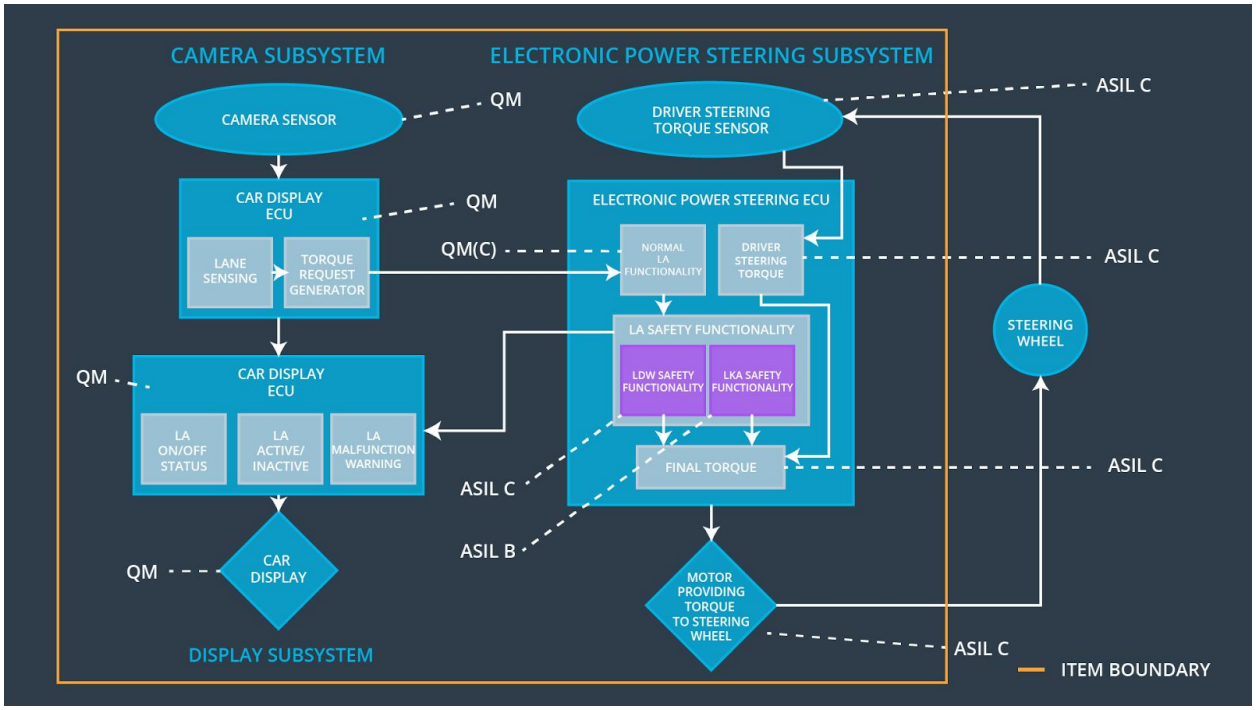
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	LKA 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	Test and validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel.	Verify that the system really does turn off if the lane keeping assistance every 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 electronic power steering ECU shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below	**X**		

01-02	Max_Torque_Frequency			
Functional Safety Requirement 02-01	The 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 functionality	Malfunction_01 Malfunction_02	Yes	Yellow light on the car display
WDC-02	Turn off LKA functionality	Malfunction_03	Yes	Yellow light on the car display