Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
May 25, 2018	1.0	Aftab Engaria	Initial Draft

Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis
- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept
- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Functional Safety Concept

The functional safety concept is a high level approach to look at the general functionality of the item without going into technical detail. The goal is to identify safety requirements and then allocate those requirements to different parts of the item architecture. From the result of the functional safety concept technical safety requirements can be derived within a subsequent technical safety concept. Functional safety requirements also have attributes that are specified in the functional safety concept. Finally, to prove that a system actually meets requirements, they have to be verified and validated.

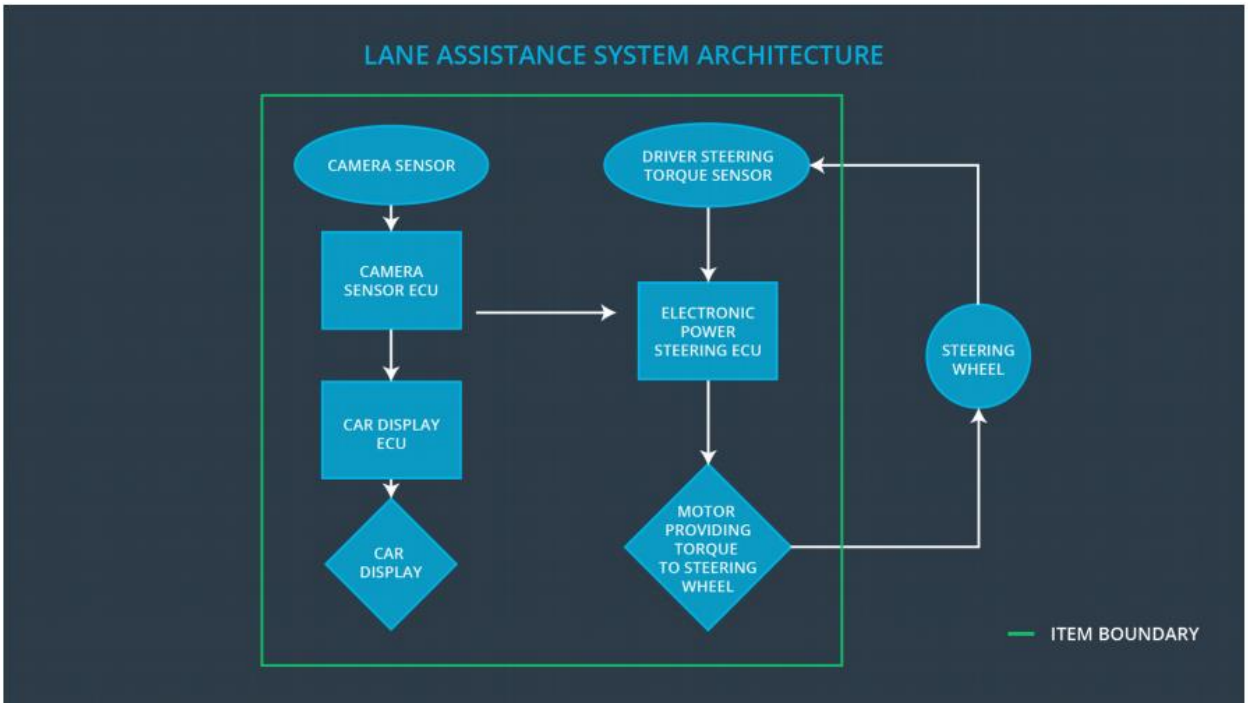
Inputs to the Functional Safety Concept

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	LKA function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver cannot misuse the system for autonomous driving
Safety_Goal_03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.

Preliminary Architecture

Following figure describes a preliminary architecture for the lane assistance item.



Description of architecture elements

Element	Description
Camera Sensor	Capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU	Analyze provided images to calculate the car position on the road respect to the road lanes.
Car Display	Provide feedback to the driver displaying warnings and the Lane Departure Assistance status.
Car Display ECU	Drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	Use the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning and request

	the necessary torque to be applied by the Motor actuator.
Motor	Applies the torque indicated by the Electronic Power Steering ECU 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

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	NO	The Lane Keeping Assistance function is not limited in time

	the steering torque when active in order to stay in ego lane		duration which lead to misuse as an lane autonomous driving function.
Malfunction_04	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	WRONG	The Lane Departure Warning start acting randomly when the camera sensor is not working.
Malfunction_05	The Lane Keeping Assistance function shall be deactivated when the camera sensor stop working.	WRONG	The Lane Keeping Assistance start acting randomly when the camera sensor is not working.

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	50ms	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	50ms	Vibration frequency is below **Max_Torque_Frequency.**
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be disabled when the camera sensor stops working.	C	10 ms	The function is disabled.

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	Appropriate values must be chosen. Validate the Max_Torque_Amplitude chosen is high enough to be detected by a driver while low enough not to cause loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Appropriate values must be chosen. Validate the Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.
Functional Safety Requirement 01-03	Validate the LDW is disabled when the camera sensor is not working.	Verify the LDW is never on when the camera sensor is not working.

Lane Keeping Assistance (LKA) Requirements:

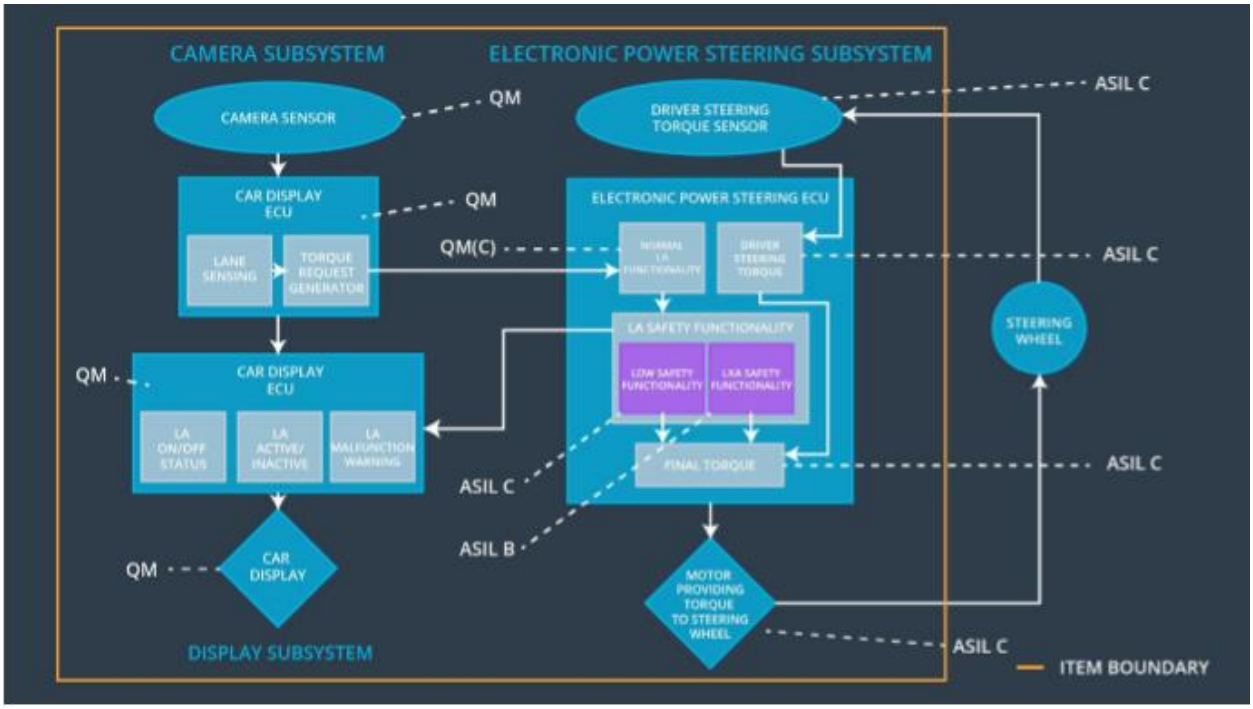
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the LKA torque is applied only Max_Duration.	B	500ms	LKA torque is zero.
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	C	10ms	Function is disabled.

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requiremen	Validate the Max_Duration chosen shall not allow the driver to use the car as a	Verify that if Lane Keeping Assistance exceeds Max_Duration, the system deactivates.

t 02-01	self-driving car.	
Functional Safety Requirement 02-02	Validate the Lane Keeping assistance shall be deactivated when the camera sensor stop working.	Verify the system does deactivate the Lane Keeping Assistance if the camera sensor is not working.

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.	**X**		

Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below	**X**		
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	**X**		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the Lane Keeping Assistance torque is applied only Max_Duration.	**X**		
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects the camera sensor is not working.	**X**		

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, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_05	Yes	Lane Keeping Assistance Malfunction Warning on Car Display