Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [1.1]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
Mar. 31, 2018	1.1	Yi-Ching Chung	First draft from the template.

Table of Contents

Purpose of the Functional Safety Concept

The system high level requirements are identified in the Functional Safety Concept documents. These requirements are allocated to different parts of the item's architecture. The technical safety requirements will be derived from these safety concepts. Instruction on how to validate and verify the requirements are presented as well.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

This is described in Table 1, quoted from the 02_HazardAnalysisAndRiskAssessment document.

Table 1 Safety Goal

ID	Safety Goal
Safety_Goal_01	The torque of oscillating steering 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.
Safety_Goal_03	The Lane Departure Warning function shall be deactivated when the camera sensor stops working.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stops working.

Preliminary Architecture

Fig.1 shows the Lane Assistance item architecture (quoted from the 01_SafetyPlan_LaneAssistance document).

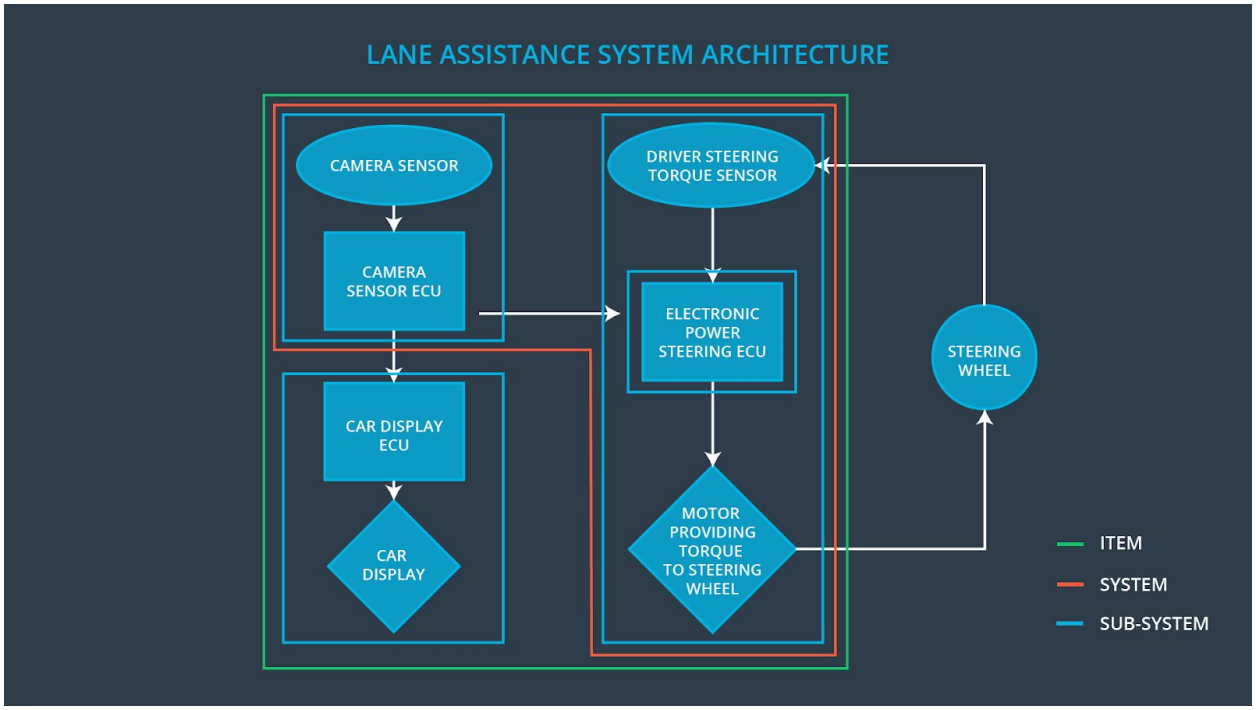

Fig. 1 Lane assistance system architecture (Udacity. *Fucntional Safety: Hazard Analysis and Risk Assessment*. Retrieved from https://classroom.udacity.com/nanodegrees/nd013/parts).

Description of architecture elements

The description and the purpose of each element in the lane assistance item are described in Table 2.

Table 2 Description for each of the item elements.

Element	Description
Camera Sensor	To capture road images and provide them to the Camera Sensor ECU.
Camera Sensor ECU	To analyze provided images to calculate the car position on the road respect to the road lanes.
Car Display	To provide feedback to the driver displaying warnings and the Lane Departure Assistance status.
Car Display ECU	To drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	To measure the torque applied to the steering wheel by the driver.

Electronic Power Steering ECU	To use the information received from the Driver Steering Torque Sensor and the torque requested by the Lane Keeping Assistance and Lane Warning; To request the necessary torque to be applied by the Motor actuator.
Motor	To apply 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

The analysis is described in Table 3.

Table 3 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	The 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	The Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide	MORE	The Lane Departure Warning function applies an oscillating torque with very high

	the driver a haptic feedback		torque frequency (above limit).
Malfunction_03	The 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 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

Table 4 and 5 describes the functional safety requirements for the lane departure warning.

Table 4 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 is 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 frequency is below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The Lane Departure Warning function shall be deactivated when the camera sensor stops working.	C	10 ms	The function is deactivated.

Table 5 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	Validate 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 exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate 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 exceeds Max_Torque_Frequency.
Functional Safety Requirement 01-03	Validate Lane Departure Warning is off when the camera sensor is not working.	Verify the Lane Departure Warning is never on when the camera sensor is not working.

Table 6 and 7 describes the functional safety requirements for the lane keeping assistance.

Table 6 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	The Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	The Lane Keeping assistance shall be deactivated when the electronic power steering ECU detects that the camera sensor is not working.	C	10 ms	The function is deactivated.

Table 7 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	To validate if the Max_Duration chosen does not allow the driver to use the car as self-driving car.	To verify if the system deactivates when the Lane Keeping Assistance torque application exceeds Max_Duration.
Functional Safety Requirement 02-02	To validate the Lane Keeping assistance shall be deactivated when the camera sensor stops working.	To verify the system does deactivate the Lane Keeping Assistance when the camera sensor is not working.

Refinement of the System Architecture

The following figure includes the system architecture with the ASIL labels.

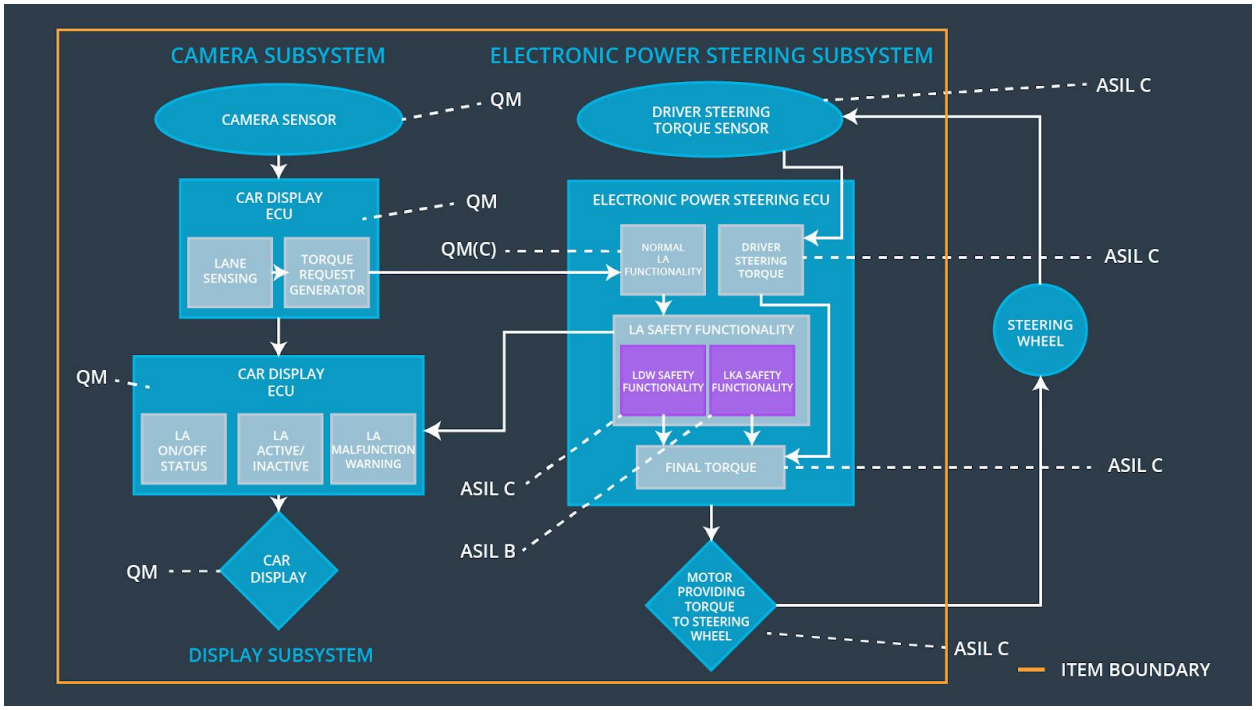

Fig 2 Refined system architecture (Udacity. *Functional Safety: Functional Safety Concept*. Retrieved from https://classroom.udacity.com/nanodegrees/nd013/parts).

Allocation of Functional Safety Requirements to Architecture Elements

Electric power steering ECU is responsible for meeting all of the requirements.

Table 8 Elements vs. functional safety requirement.

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	The Lane Departure Warning	**X**		

Safety Requirement 01-02	item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.			
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

Table 9 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