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
05/22/2018	1.0	Swapnil More	First Draft
06/15/2018	1.1	Swapnil More	Updates to First Draft

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the functional safety concept is to look at the item from a high-level perspective, refine the safety goals from hazard analysis and risk assessment as functional safety requirements, allocate safety requirements to the relevant parts of the system diagram; and discuss the verification, validation i.e. how to prove that the system actually meets the requirements.

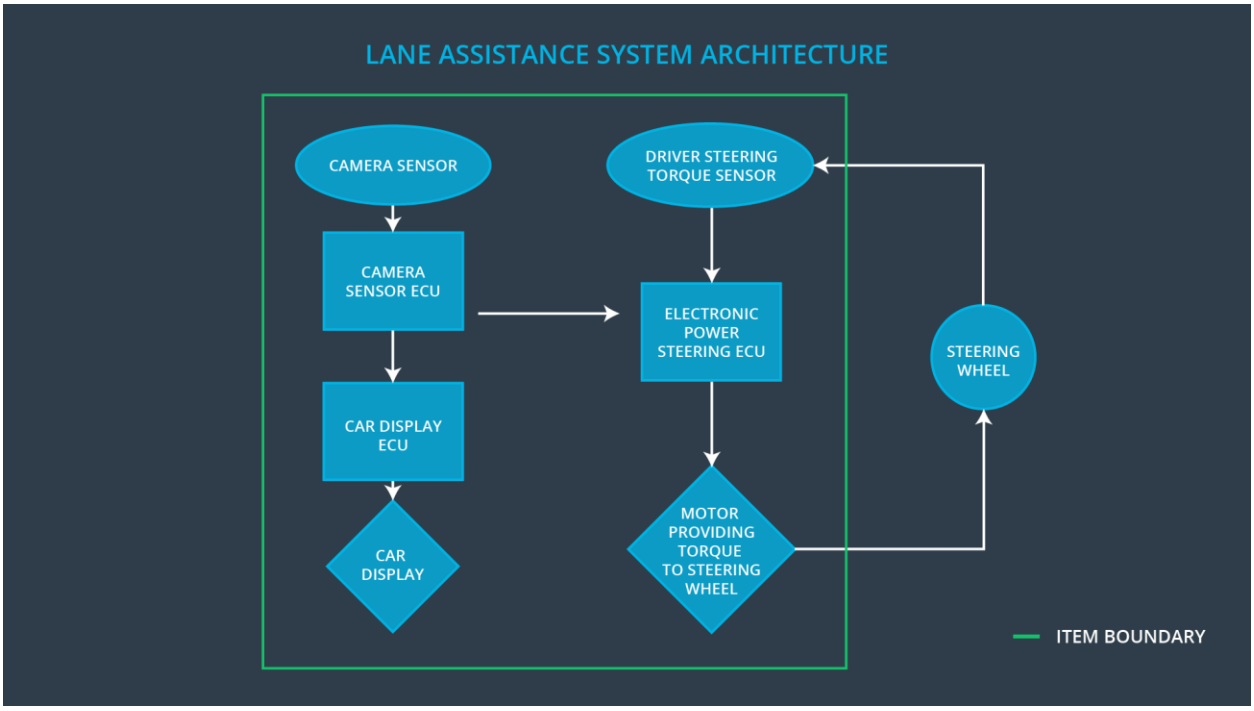
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel from the lane keeping assistance 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 Assistance provided by the Lane Keeping System shall be limited.
Safety_Goal_04	The Lane Keeping Assistance function shall be deactivated when the camera sensor stops working.

Preliminary Architecture

The lane assistance item preliminary architecture:



Description of architecture elements

Element	Description
Camera Sensor	Capture images and send them to the Camera Sensor ECU
Camera Sensor ECU	Process images to detect lane lines, calculate the vehicles position with respect to the lane lines and send information to the EPS ECU
Car Display	Display the Lane Departure Warning and status of the Lane Assistance System
Car Display ECU	Control the car display based on inputs from the camera sensor ECU
Driver Steering Torque Sensor	Measure Steering Wheel Torque
Electronic Power Steering ECU	Calculate the assistance torque, motor torque based on inputs from the camera sensor ECU
Motor	Generate torque requested 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 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.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active to stay in ego lane	MORE	The Lane Keeping Assistance applies a torque with very high torque amplitude (above limit)
Malfunction_05	Lane Departure	WRONG	The Lane

	Warning (LDW) function shall apply an oscillating steering torque to provide the driver with haptic feedback		Departure Warning 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	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 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	50 ms	Camera sensor status is active.

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 exceeded 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 exceeded 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.

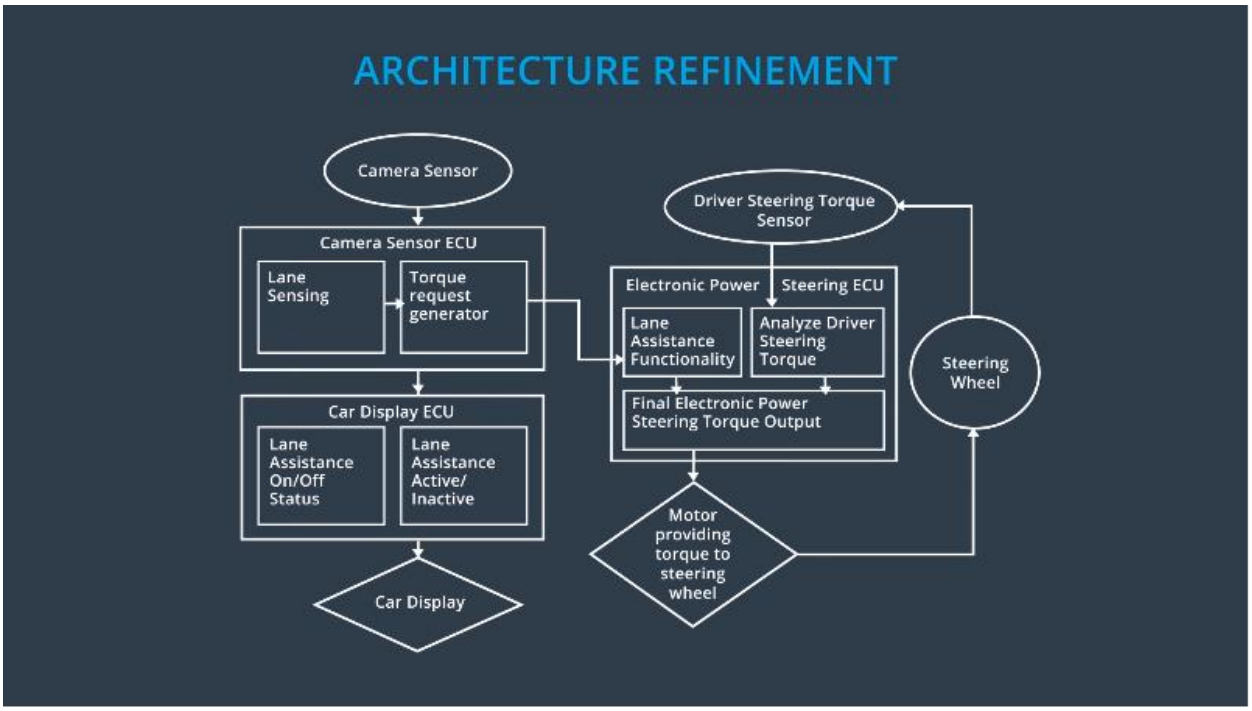
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The Lane Keeping Assistance item shall ensure that the time duration for steering assistance is below Max_Assist_Time	B	500 ms	Assistance time is below Max_Assist_Time
Functional Safety Requirement 02-02	The Lane Keeping Assistance item shall ensure that the lane assist torque amplitude is below Max_Assist_Amplitude.	C	50 ms	Assistance torque amplitude is below Max_Assist_Torque

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 Max_Assist_Time chosen is adequate to provide required assistance but not long enough for the driver to misuse the system	Verify the system does turn off if the Lane Keeping Assistance exceeded Max_Assist_Time
Functional Safety Requirement 02-02	Validate Max_Assist_Amplitude chosen is adequate to provide required assistance and not cause the loss of steering	Verify the system does turn off if the Lane Keeping Assistance exceeded Max_Assist_Amplitude

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 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement 01-03	The Electronic Power Steering ECU shall deactivate the Lane Departure Warning function	**X**		

	when the camera sensor stops working.			
Functional Safety Requirement 02-01	The Electronic Power Steering ECU shall ensure that the time duration for steering assistance is below Max_Assist_Time	**X**		
Functional Safety Requirement 02-02	The Electronic Power Steering ECU shall ensure that the lane assist torque amplitude is below Max_Assist_Amplitude.	**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_05	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03, Malfunction_04	Yes	Lane Keeping Assistance Malfunction Warning on Car Display