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
01.04.2018	1.0	Siddarth Kothiwale	First Trial

Table of Contents

Purpose of the Functional Safety Concept

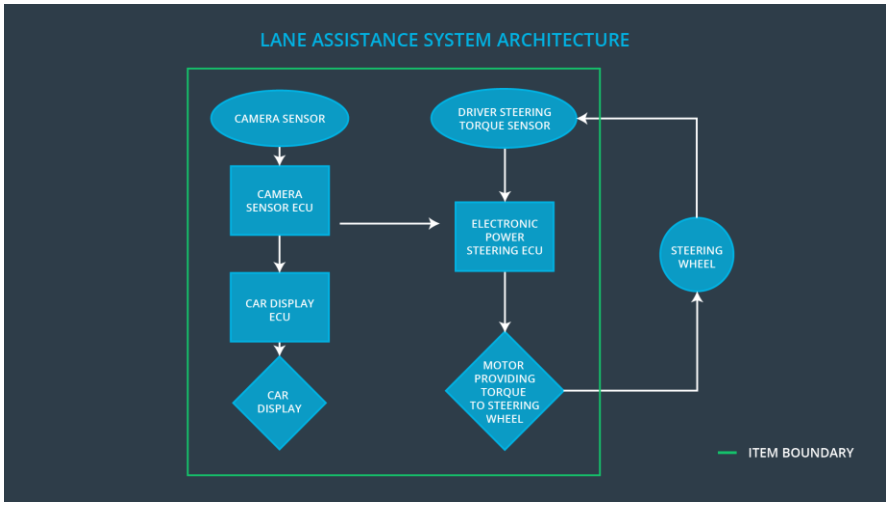
The functionalional safety concept looks at item from higher level without going too deep in technicalities.
We need to allocate these safety requirements to the relevant parts of the system diagram. Allocation means defining which part of the system architecture will implement each requirement. This could involve expanding the system architecture with new element blocks. We will then refine the system architecture to handle the new requirements.
This all information is handled in Functional safety concept.

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 time interval so that the driver cannot misuse the systema for autonomous driving

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	To record the video of the road ahead
Camera Sensor ECU	To process the video from Camera Sensor and detect the lane lines
Car Display	To Display the warnings such as lane departure
Car Display ECU	Car Display processes the input from the Camera sensor ECU and provides different warnings
Driver Steering Torque Sensor	It detects the torque that the driver is providing
Electronic Power Steering ECU	The ECU calculates the necessity and the amount of torque that needs to be provided to keep the car in the lane
Motor	The Motor is the actuator here. It takes the input from the ECU and then provides the required 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

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
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
Malfunction_03	Lane Keeping	NO	The lane keeping

	Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane		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	50 ms	Set System torque to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Set System torque to 0

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. Method: test inserting a fault into the system and seeing what happens.
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. Method: 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	Set System torque to 0

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	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 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 frequency is	x		

	below 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 the function	Amplitude> Max_Torque_Amplitude and Frequency> Max_Torque_Frequency	Yes	Warning sign in driver display system
WDC-02	Turn off the function	If LKA active for time > Max_Duration	Yes	Warning sign in driver display system