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
2018.05.26	1.0	A. Fuchs	Initial revision

Table of Contents

Purpose of the Functional Safety Concept

The purpose of the Functional Safety Concept is to refine the high level safety goals from the HARA into Functional Safety Requirements. It looks at the general functionality of the item.

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 system for autonomous driving.
Safety_Goal_03	The reaction time of the LKA function shall not exceed a defined threshold.
Safety_Goal_04	Unexpected high oscillating torque shall be prevented.

Preliminary Architecture

Description of architecture elements

Element	Description
Camera Sensor	Provide picture input of the actual driving condition.
Camera Sensor ECU	Lane sensing and request torque generation.
Car Display	Give visual outputs to the driver to inform or warn him of current system states.
Car Display ECU	Set the status of the lane assistance function in terms of on/off or active/inactive.
Driver Steering Torque Sensor	Measuring of the steering torque of the steering wheel.
Electronic Power Steering ECU	Analyze the driver steering torque, provide lane assistance functionality, output the final electronical power steering torque request.
Motor	Generate and provide steering 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 (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 oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Turn off LDW function.
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Turn off LDW function.

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 if the value for Max_Torque_Amplitude is chosen appropriate by testing different drivers' reaction to different torque amplitudes.	Software test by inserting a fault into the system and test if the torque output is 0Nm within the 50ms FTTI.
Functional Safety Requirement 01-02	Test if the value for Max_Torque_Frequency is chosen appropriate by testing different drivers' reaction to different torque frequencies.	Software test by inserting a fault into the system and test if the torque output is 0Nm within the 50ms FTTI.

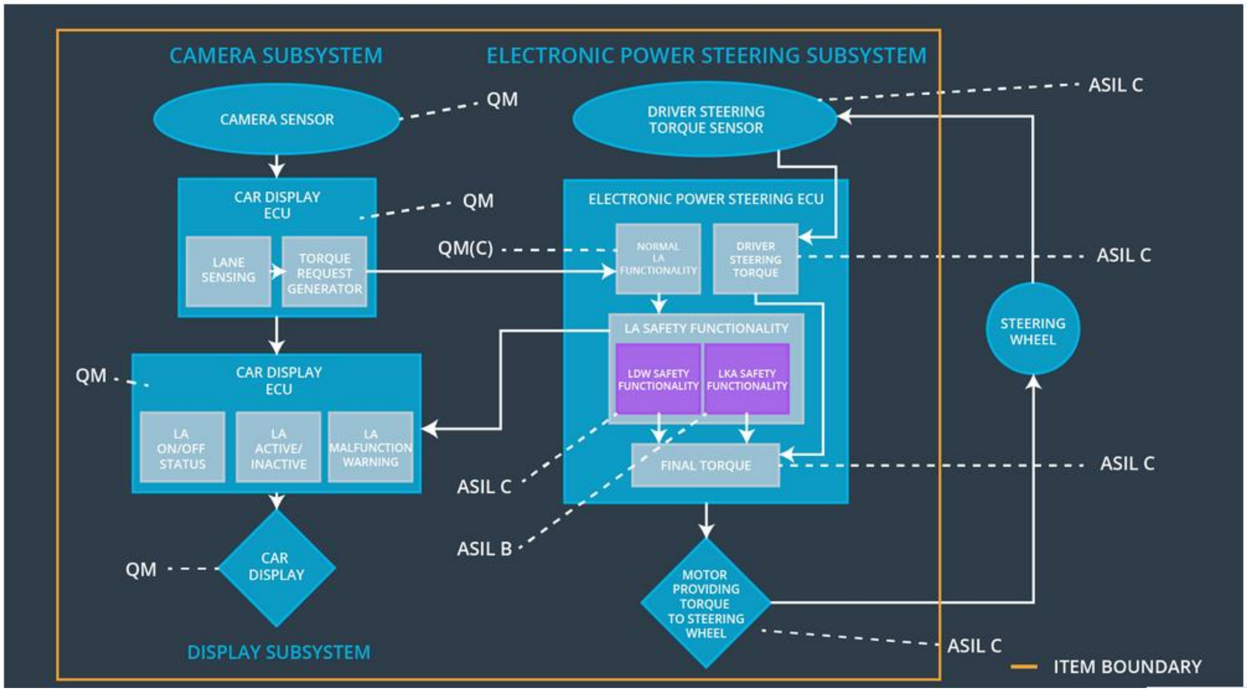
Lane Keeping Assistance (LKA) Requirements:

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	500ms	Turn off the LKA function.

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 if the value for Max_Duration dissuades drivers from taking their hands off the wheel.	Test if the system turns off if the lane keeping assistance exceeds 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 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 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 system.	Torque amplitude is higher than Max_Torque_Amplitude	Yes	Warning lamp at the vehicle dashboard.
WDC-02	Turn off the system.	Torque frequency is higher than Max_Torque_Fr	Yes	Warning lamp at the vehicle dashboard.

		equency		
WDC-03	Turn off the system.	Duration of torque application is higher than ‘Max_Duration’	Yes	Warning lamp at the vehicle dashboard.