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
26.03.2018	0.1	Stefan Cyliax	Initial version for functional safety project
01.04.2018	1.0	Stefan Cyliax	First RC

Table of Contents

Contents

Purpose of the Functional Safety Concept

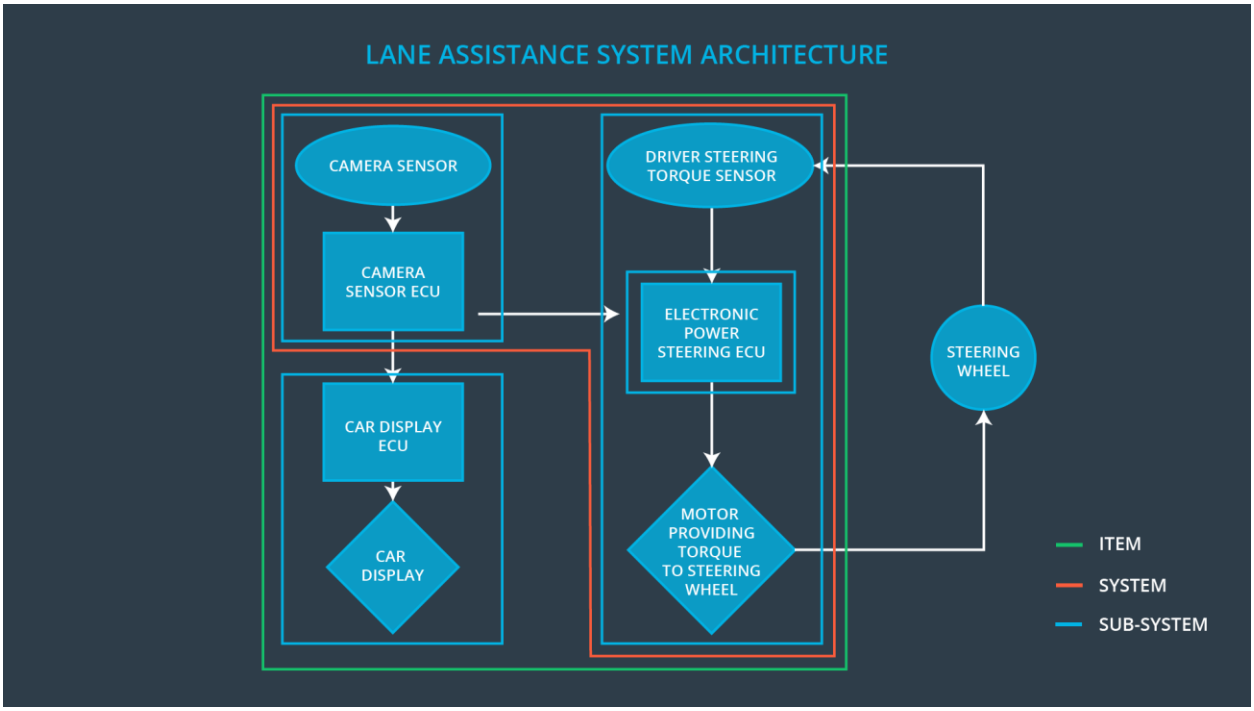
The purpose of the Functional Safety Concept is to derive general hardware and software requirements that mitigate the identified risks on the level of sensors, control units and actuators. The requirements are then allocated to the system architecture. This could involve expanding the system architecture with new element blocks.

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 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.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Records images of the road ahead of the vehicle.
Camera Sensor ECU	Detects lane lines on the images, derives position and direction of vehicle relative to the lane and generates torque request.
Car Display	Informs the driver about the state of the function.
Car Display ECU	Process information for display to the driver.
Driver Steering Torque Sensor	Senses steering operation of the driver.
Electronic Power Steering ECU	Implements the logic behind both lane assistance systems. Processes the inputs from the Camera Sensor ECU and Driver Steering Torque Sensor and controls the Motor that provides torque to the steering wheel.
Motor	Can provide 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 lane keeping item shall ensure that the lane departure oscillation torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Gradually reduce steering torque to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillation torque frequency is below Max_Torque_Frequency.	C	50 ms	Gradually reduce steering torque to zero

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 that the chosen Max_Torque_Amplitude is manageable for a normal driver.	Test that the limiting to Max_Torque_Amplitude works regardless of the input.

Functional Safety Requirement 01-02	Test that the chosen Max_Torque_Frequency is manageable for a normal driver.	Test that the limiting to Max_Torque_Frequency works regardless of the input.

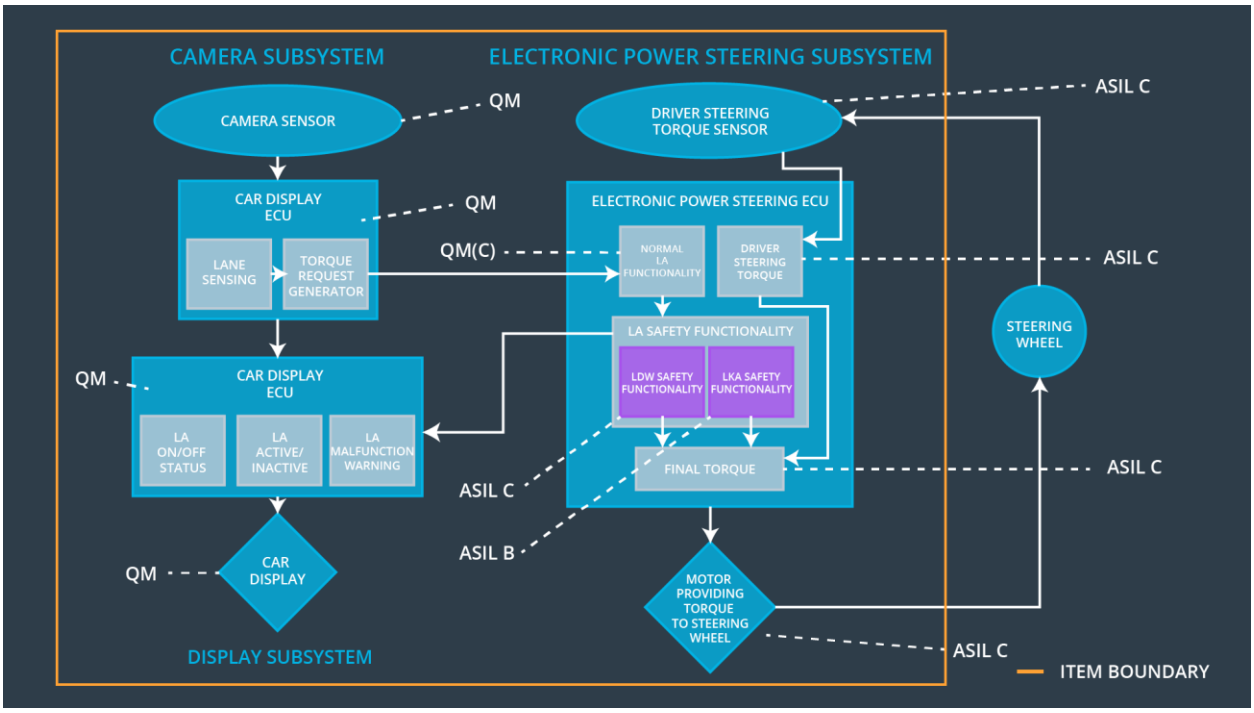
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	Gradually reduce steering torque to zero

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 that the max_duration chosen really did dissuade drivers from taking their hands off the wheel.	Test that the function turns off after 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 oscillation torque amplitude is below Max_Torque_Amplitude.	**x**		
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillation torque frequency is below Max_Torque_Frequency.	**x**		
Functional Safety	The Electronic Power Steering ECU shall ensure that the lane	**x**		

Requirement 02-01	keeping assistance torque is applied for only Max_Duration.			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Function off	Torque above limit	Yes	Warning on car display
WDC-02	Function off	Time limit exceeded	Yes	Warning on car display