Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 3.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
18.03.2018	1.0	P. Schalast	Initial commit
31.03.2018	2.0	P. Schalast	Review for project commit
02.04.2018	3.0	P. Schalast	Minor changes

Table of Contents

Purpose of the Functional Safety Concept

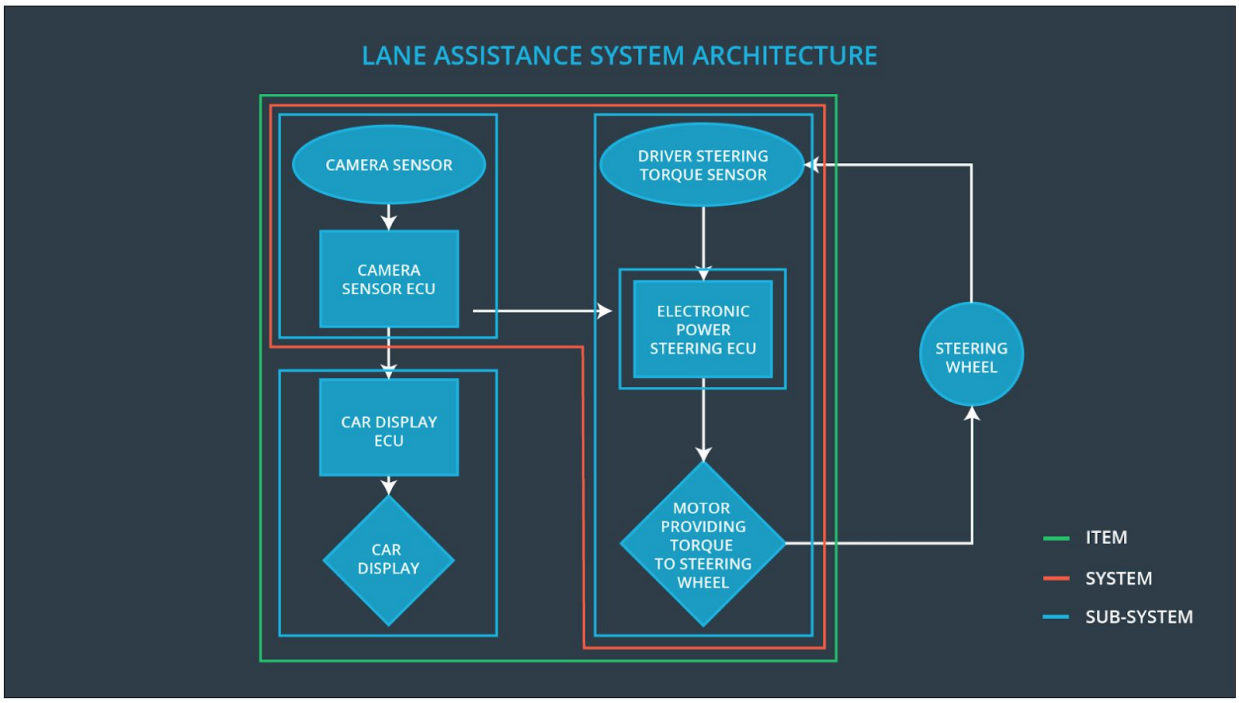
The functional safety concept identifies new requirements and allocates these requirements to system diagrams at the item from a higher level.

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.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Capture images from the road ahead and provide to the Camera Sensor ECU
Camera Sensor ECU	Detect lane lines in the received images, derive position and direction of the vehicle relative to the lanes and generate correction torque request
Car Display	Display warnings and information
Car Display ECU	Process information to be shown on the display
Driver Steering Torque Sensor	Measure torque set by the driver
Electronic Power Steering ECU	Receive information from the Driver Steering Torque Sensor and the Camera Sensor ECU to derive the required torque to be applied to the motor
Motor	Apply final torque for vehicle steering

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	MORE	The lane departure warning function applies an oscillating torque with very high torque amplitude

	driver a haptic feedback		(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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Gradually reduce steering 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	Gradually reduce steering torque to 0

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance	Verification Acceptance

	Criteria and Method	**Criteria and Method**
Functional Safety Requirement 01-01	Test that Max_Torque_Amplitude is reasonable and manageable by driver	Limiting Max_Torque_Amplitude works regardless of the input
Functional Safety Requirement 01-02	Test that Max_Torque_Frequency is reasonable and manageable by driver	Limiting Max_Torque_Requency works regardless of the input

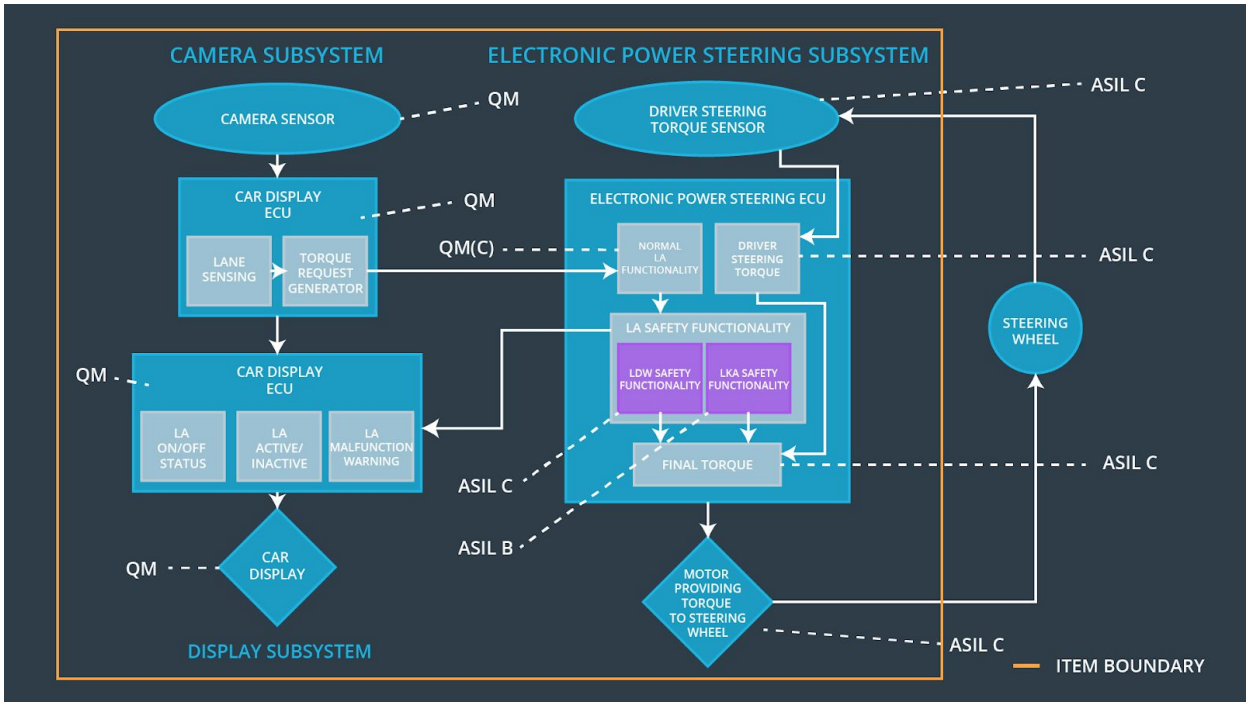
Lane Keeping Assistance (LKA) Requirements:

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 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	Test and validate that the Max_Duration chosen really did dissuade drivers from taking their hands off the wheel	Test that 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 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 functionality	Torque above limit	Yes	Warning via car display
WDC-02	Turn off the functionality	Time limit exceeded	Yes	Warning via car display