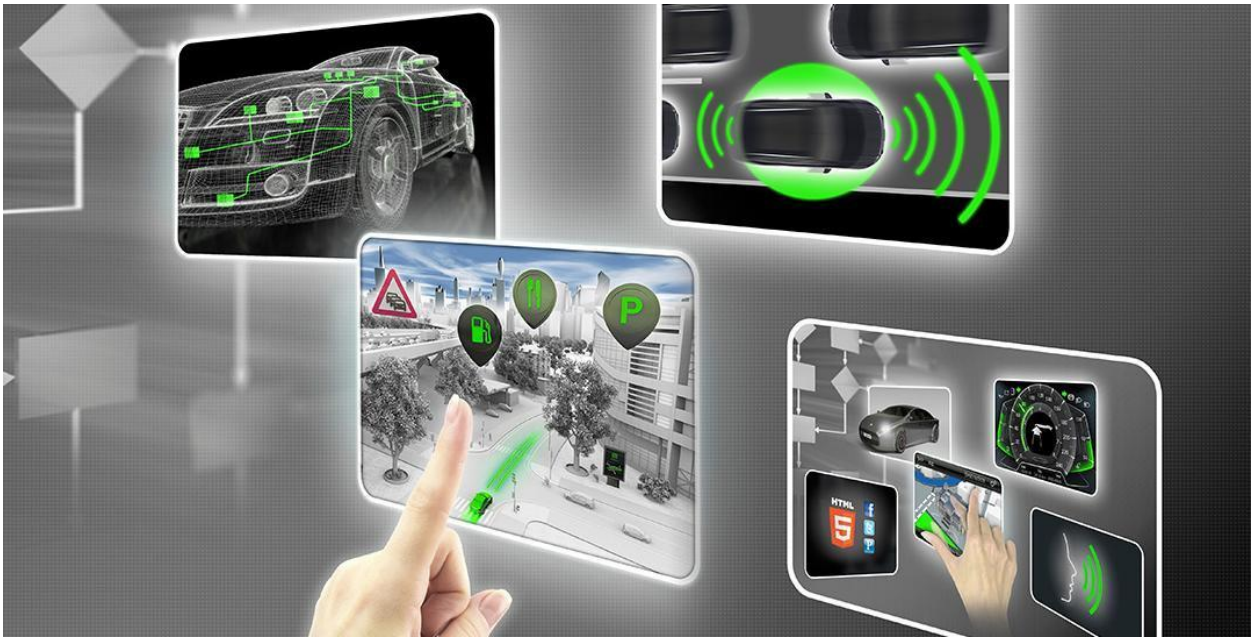
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Version 1.0, Released on 2018-05-21



Document history

Date	Version	Editor	Description
2018-05-21	1.0	Navin Rawther	Initial Draft

Table of Contents

Purpose of the Functional Safety Concept

The Functional Safety Concept refines the safety goals into functional safety requirements and allocates these safety requirements to the relevant parts of the system diagram. The system architecture is refined to handle the new requirements. These are done on a bird’s eye view, ie, on an overall level.

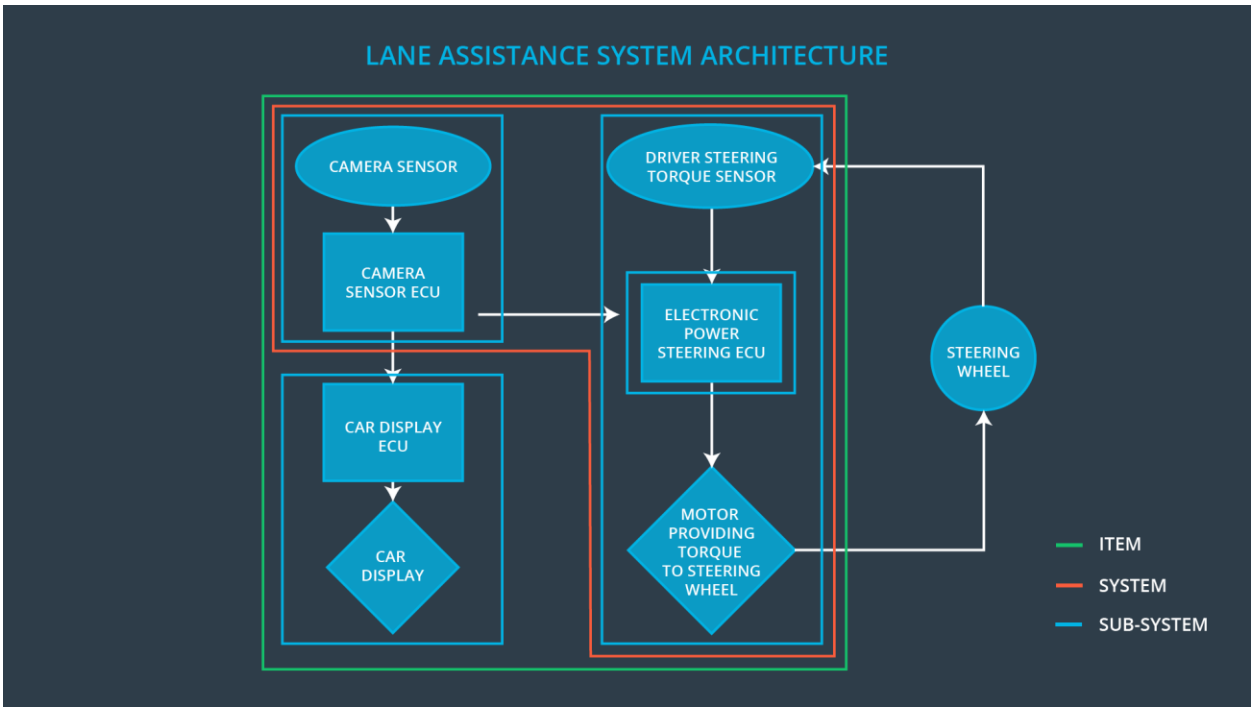
Inputs to the Functional Safety Concept

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

The following figure shows the lane assistance system architecture.



The main system of the item contains the camera subsystem and the steering subsystem with a display subsystem outside of the system. The steering wheel actually lies outside the item.

Description of architecture elements

Element	Description
Camera Sensor	Captures the images of the road to identify lane lines
Camera Sensor ECU	Contain the hardware and software required for deep learning and computer vision techniques used for identification of lane lines and calculation of vehicle's position in the lane
Car Display	Contains the warning light to indicate lane assistance system is active
Car Display ECU	Contain the hardware and software to enable the car display and to share information between the camera subsystem and the car display subsystem
Driver Steering Torque Sensor	Detects how much the steering wheel is already turned
Electronic Power Steering ECU	Contain hardware and software to provide commands to turn and vibrate the steering wheel. It also communicates with the camera subsystem
Motor	Provides torque to the steering wheel to obtain the required 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 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 warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Lane departure warning oscillating amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequeny is below Max_Torque_Frequency	C	50ms	Lane departure warning oscillating torque frequency is below Max_Torque_Frequency

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	A Max_Torque_Amplitude has to be chosen and validated that it is a reasonable value by testing how drivers react to different torque amplitudes and chosing the comfortable one	Verify that lane assistance output is zero within the 50ms fault tolerant time interval for the chosen Max_Torque_Amplitude
Functional Safety Requirement 01-02	A Max_Torque_Frequency has to be chosen and validated that it is a reasonable value by testing how drivers react to different torque frequencies and chosing the comfortable one	Verify that lane assistance output is zero within the 50ms fault tolerant time interval for the chosen Max_Torque_Frequency

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASI	Fault Tolerant Time	Safe State

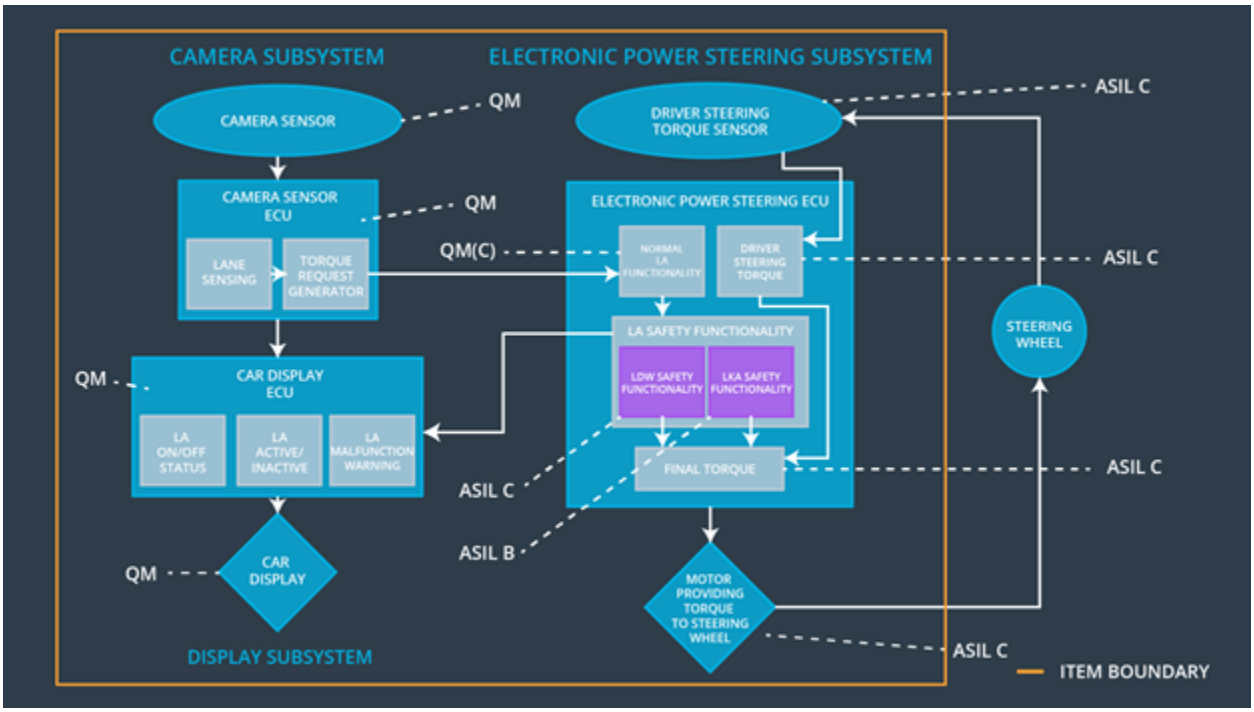
		L	Interval	
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500ms	Lane keeping assistance torque is 0 after Max_Duration

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 dissuades drivers from taking their hands off the wheel	Verify that the Lane Keeping Assistance function turned off every exceeded Max_Duration

Refinement of the System Architecture

The figure below shows the refined system architecture with the ASIL values:



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 warning 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 warning oscillating torque frequeny 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	Lane Departure Warning functionality is turned off	Malfunction_01, Malfunction_02	Yes	Lane Assistance Warning light in driver dashboard turned on
WDC-02	Lane Assistance function turned off	Malfunction_03	Yes	Lane Assistance Warning light in driver dashboard turned on