



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
Jan 04 2018	1.0	Tarun Kandala	First draft/submission
Jan 6 th 2018	1.1	Tarun Kandala	Revised based on feedback

Table of Contents

[Document history](#)

[Table of Contents](#)

[Purpose of the Functional Safety Concept](#)

[Inputs to the Functional Safety Analysis](#)

[Safety goals from the Hazard Analysis and Risk Assessment](#)

[Preliminary Architecture](#)

[Description of architecture elements](#)

[Functional Safety Concept](#)

[Functional Safety Analysis](#)

[Functional Safety Requirements](#)

[Refinement of the System Architecture](#)

[Allocation of Functional Safety Requirements to Architecture Elements](#)

[Warning and Degradation Concept](#)

Purpose of the Functional Safety Concept

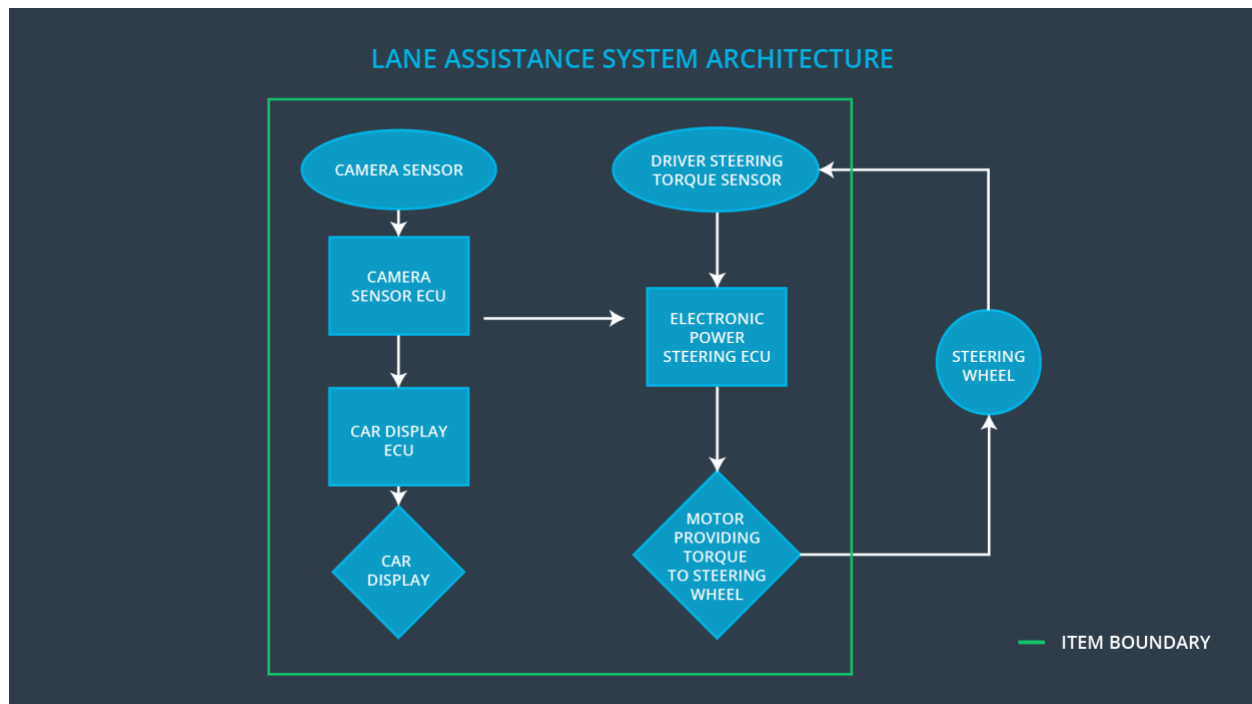
Purpose of the Functional Safety Concept is to identify new requirements and allocate these requirements to system diagrams at a general functionality level.

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	Responsible for detecting lanes
Camera Sensor ECU	Responsible for determining when the vehicle leaves the lane by mistake
Car Display	Display lane departure warning
Car Display ECU	Manage the display warnings
Driver Steering Torque Sensor	Sense the torque applied by the driver
Electronic Power Steering ECU	Combine the sensor readings from the Driver Steering Torque sensor and Camera Sensor to decide how much resultant torque to apply to steering
Motor	Apply the resultant 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 oscillating amplitude is too high

Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The oscillating frequency is too high
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	50ms	LDW Torque Request Amplitude shall be set to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	LDW Torque Request Frequency shall be set 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 how drivers react to different torque amplitudes to prove that we chose an appropriate value	Perform software test inserting a fault into the system and verify when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	test how drivers react to different torque frequencies to prove that we chose an appropriate value	Perform software test inserting a fault into the system and verify when the torque Frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

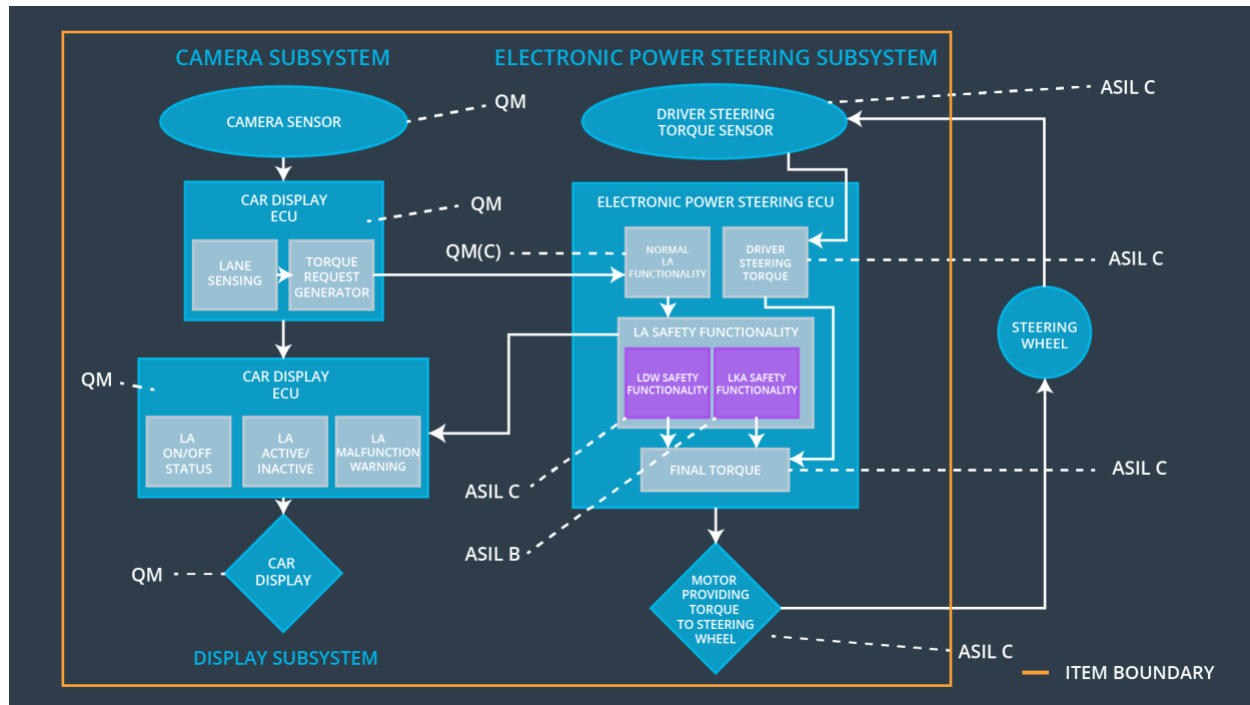
Lane Keeping Assistance (LKA) Requirements:

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	LKA Torque Request shall be set 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 and validate that 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 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 Lane Departure warning function	When the oscillating torque amplitude and frequency go beyond limit	Yes	The driver will see a warning light on the dashboard when the system malfunctions
WDC-02	Turn off Lane Keeping assistance function	When the lane keeping assistance goes beyond the set time limit	Yes	The driver will see a warning light on the dashboard when the system malfunctions