



Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
05/12/18	1.0	Diogo Leal	First submission

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

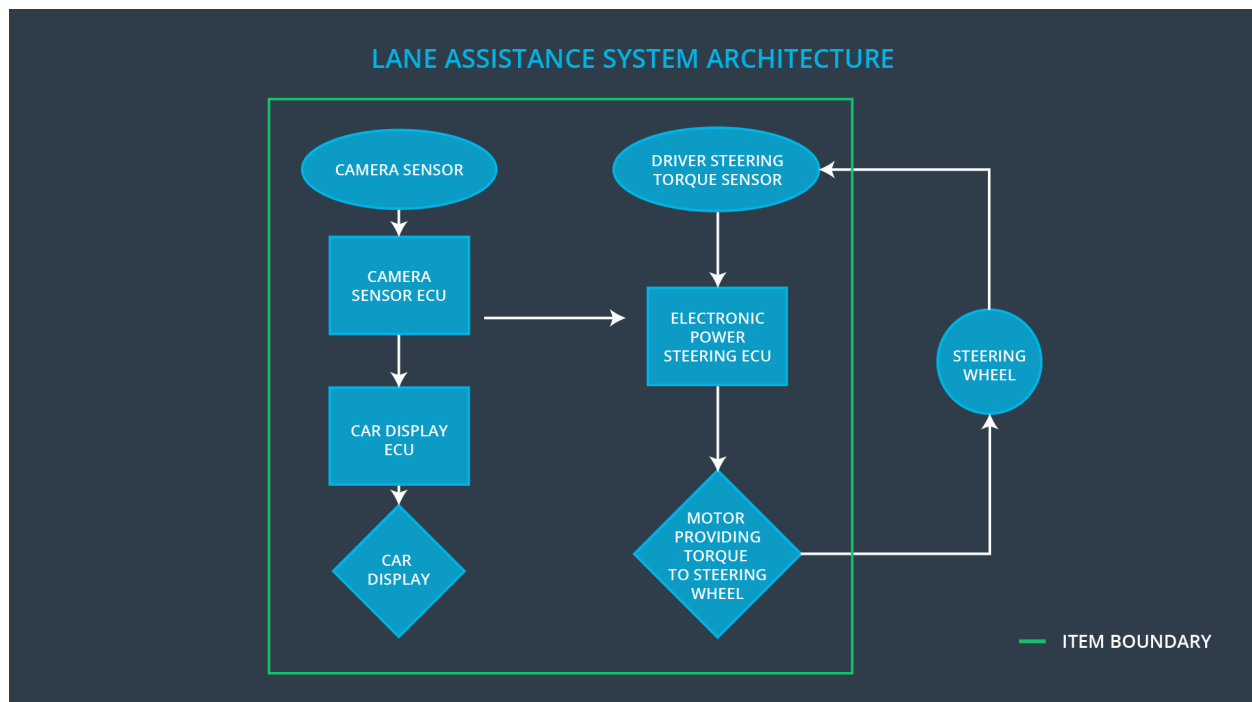
The purpose of the Functional Safety Concept is to refine the safety goals in what are called functional safety requirements looking at the general functionality of the item.

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

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Responsible for detecting lane lines
Camera Sensor ECU	Determines when the vehicle leaves the lane by mistake
Car Display	Alerts the driver if the system is on/off, active/inactive and if a fault has occurred
Car Display ECU	Treats the information from the EPS to display to the driver
Driver Steering Torque Sensor	Responsible for measuring the torque provided by the driver
Electronic Power Steering ECU	Adds an appropriate amount of torque based on a lane assistance system torque request
Motor	Moves 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	A S I L	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	Oscillating torque from LDW function is 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	Oscillating torque from LDW function is 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 the value chosen for the torque amplitude	Verify that the the lane assistance output is set to zero within the 50 ms when the torque amplitude is higher than the value chosen during validation
Functional Safety Requirement 01-02	Test how drivers react to the value chosen for the torque frequency	Verify that the the lane assistance output is set to zero within the 50 ms when the torque frequency is higher than the value chosen during validation

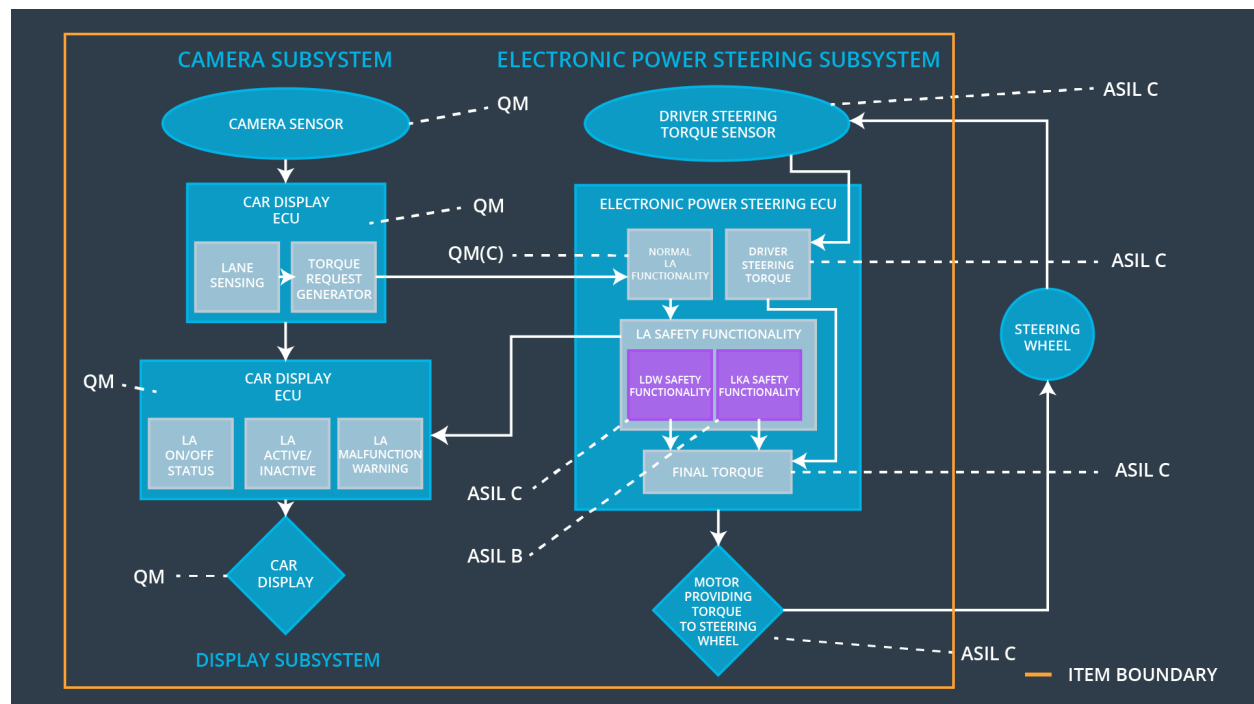
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	A S I L	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	Torque request from the LKA function is 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 if the maximum duration chosen really dissuade drivers from taking their hands off the wheel	Verify that the system really does turn off if the lane keeping assistance is active for a period bigger than the maximum 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 the functionality	The lane departure warning function applies an oscillating torque with very high torque frequency or amplitude (above limit)	Yes	Warning light on the dashboard
WDC-02	Turn off the functionality	The lane keeping function torque is applied for a very long period (above limit)	Yes	Warning light on the dashboard