Functional Safety Concept Lane Assistance

Document Version: 1.0
08.04.2018

Document history

Date	Version	Editor	Description
08.04.2018	1.0	GRANIE Guillaume	First Attempt

Table of Contents

Purpose of the Functional Safety Concept

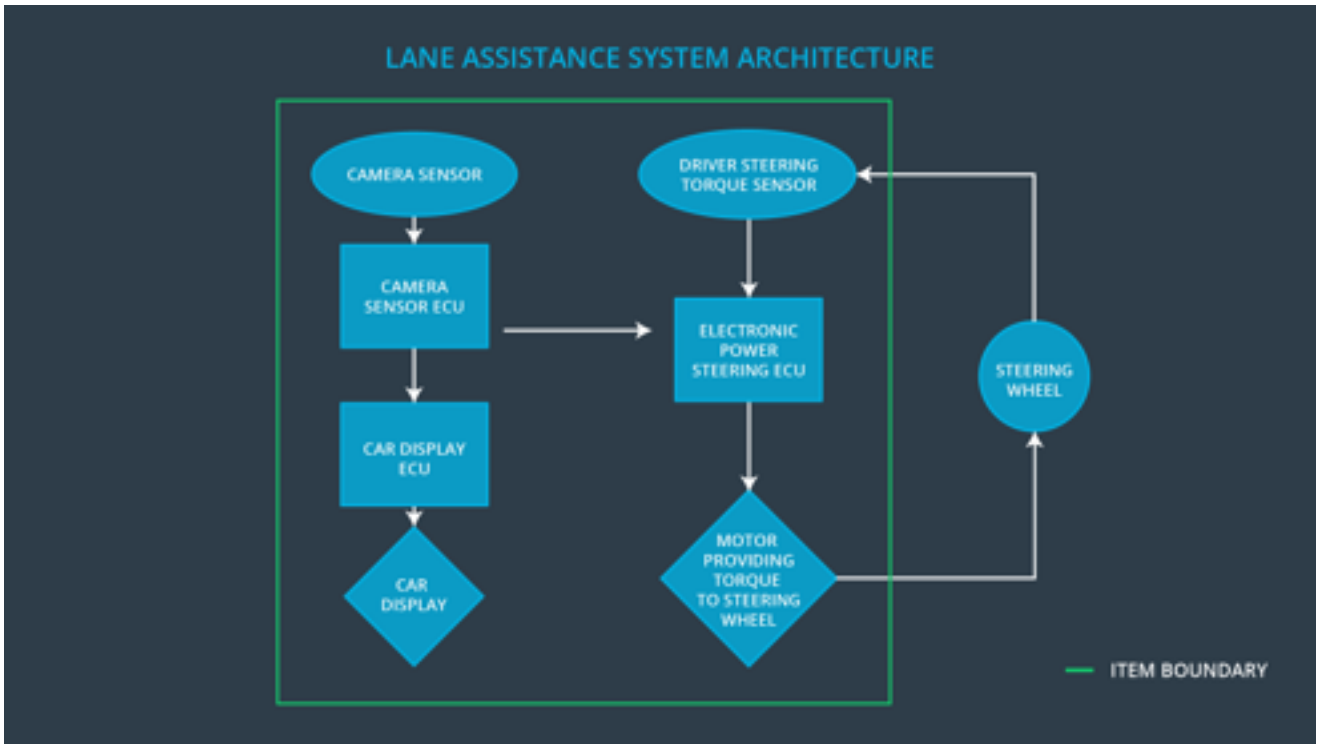
The functional safety concept provides a high level overview of the system. Based on the hazard analysis and risk assessment, it details what the system is required to do in order to reduce risks involved by the Lane Assistance functionality to acceptable levels. It considers the system as a black box and only defines how it should behave from an exterior point of view without any knowledge of the specific implementation.
This document also specifies instructions about how to verify and validate the requirements.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The amplitude of the oscillating steering torque from the Lane Departure Warning function shall be limited and could never exceed a defined safety threshold.
Safety_Goal_02	The LKA function shall be time limited to keep the driver focused on the driving task.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Forward facing sensor collecting images.
Camera Sensor ECU	Image processing unit responsible for detecting the lane lines and deriving from them a corrected steering to the electronic power steering ECU as well as warning messages to the car display ECU.
Car Display	Screen responsible for displaying informational and warning messages to the driver.
Car Display ECU	Processing unit responsible for interpreting the messages received from the camera sensor ECU and producing the corresponding visual clues on the car display.
Driver Steering Torque Sensor	Sensor responsible for measuring the amount of torque applied by the driver to the steering wheel in both rotational directions.
Electronic Power Steering ECU	Processing unit responsible for interpreting the steering torque request from the electronic power steering ECU and producing the according signals to the motor.
Motor	Actuator responsible for issuing 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 has no duration limit and could be interpreted 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Frequency.	C	50ms	Vibration torque amplitude 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	Validation that Max_Torque_Amplitude is appropriate and won't cause panic nor vehicle control loss.	Verify through thorough testing that the applied vibration torque amplitude does not exceeds Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validation that Max_Torque_Frequency is appropriate and won't cause panic nor vehicle control loss.	Verify through thorough testing that the applied vibration torque frequency does not exceeds Max_Torque_Frequency.

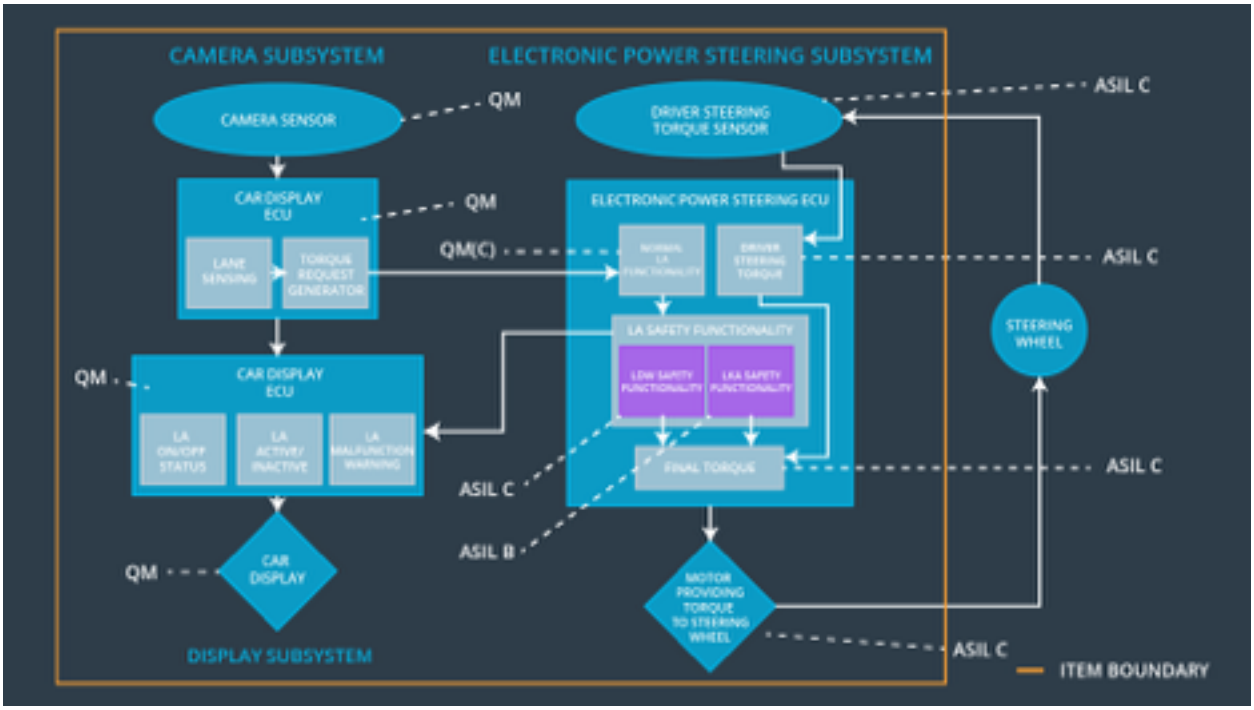
Lane Keeping Assistance (LKA) Requirements:

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 only during a duration equals to Max_Duration after manual activation by the driver.	B	500ms	Lane Keeping Assistance torque is null.

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	Validation that Max_Duration is not too long nor too short for the driver to keep focus on the driving task and not lose attentiveness.	Verify through thorough testing that the Lane Keeping Assistance activation period does not exceeds 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 Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	X		
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude 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 only during a duration equals to Max_Duration after manual activation by the driver.	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_02	Yes	Dashboard signal
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Dashboard signal