Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0 Released 2017-12-26

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12/26/2017	1.0	Daniel Prado	Initial version

Table of Contents

Purpose of the Functional Safety Concept

The Functional Safety Concept document is part of the safety process of ISO 26262 for the treatment of potential malfunctions in electrical and electronic systems.

Its main purpose is to refine the functional safety goals into functional safety requirements and allocate them to appropriate place in the System items architecture, and also expanding the system architecture with new element blocks if deemed necessary.

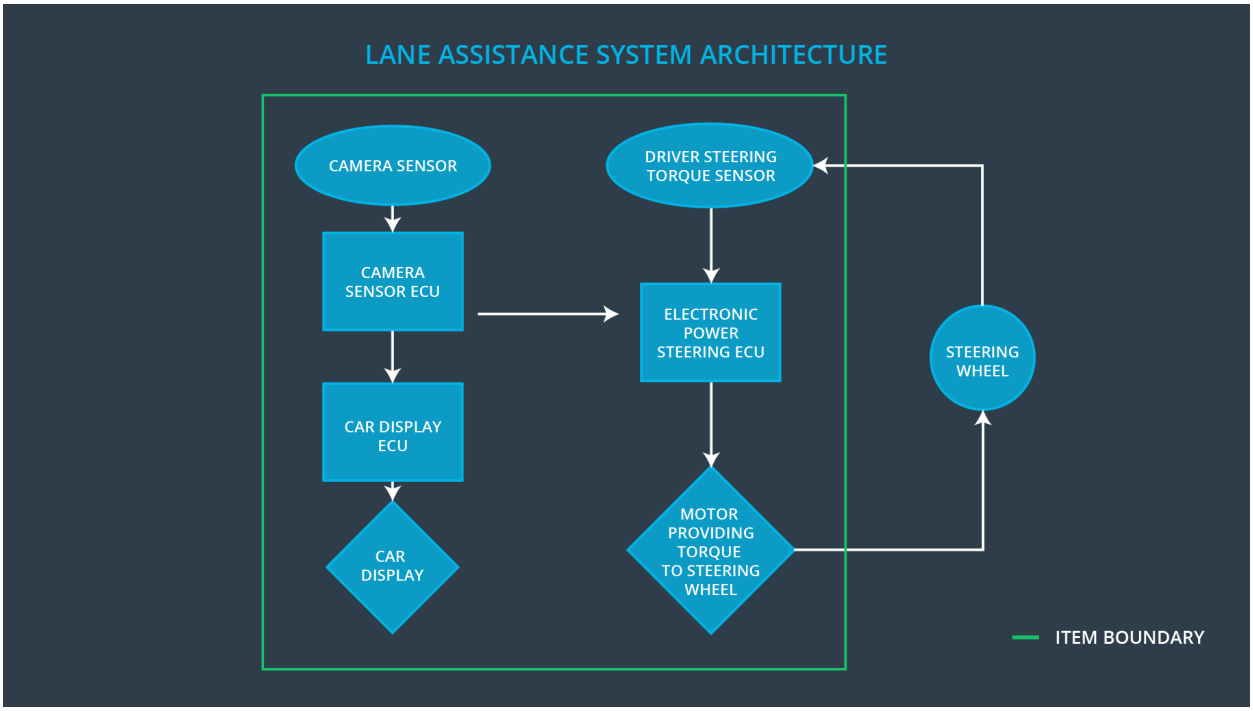
Inputs to the Functional Safety Concept

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 image presents the preliminary architecture, which will be refined in this document.



Description of architecture elements

Element	Description
Camera Sensor	Sensor for the optical detection of the front area of the vehicle, including detectable lane lines.
Camera Sensor ECU	Electronic Control Unit (ECU) responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Responsible for triggering reactions to add extra torque for LDW and LKA functionality.
Car Display	Visual display which is, among other functionalities, responsible for displaying warning of lane departures and displaying LKA and LDW status.
Car Display ECU	Electronic Control Unit (ECU), which is responsible for creating and providing the data and information that the car display visualizes.
Driver Steering Torque Sensor	Sensor responsible for measuring the steering torque provided by the driver.
Electronic Power Steering ECU	Electronic Control Unit (ECU) responsible for evaluating the torque provided by the driver and for adding an additional torque based on the torque request of the lane assist system (LKA). Initializes the

	vibration of the steering wheel when the driver inadvertently drifts away from the center of the lane (LDW).
Motor	Device that adds extra 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 DV04 - Actor effect is too much (torque amplitude)	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 DV04 - Actor effect is too much (torque frequency)	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 DV03 - Function always activated	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	Set the oscillating torque 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	Set the oscillating torque 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	Validate that Max_Torque_Amplitude is chosen high enough that the driver notices it but low enough not to cause loss of steering.	Verify that the system really sets oscillating torque to zero if the lane departure warning ever causes a vibration above Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate that Max_Torque_Frequency is chosen high enough that the driver notices it but low enough not to cause loss of steering.	Verify that the system really sets oscillating torque to zero if the lane departure warning ever causes a vibration above Max_Torque_Frequency.

Lane Keeping Assistance (LKA) Requirements:

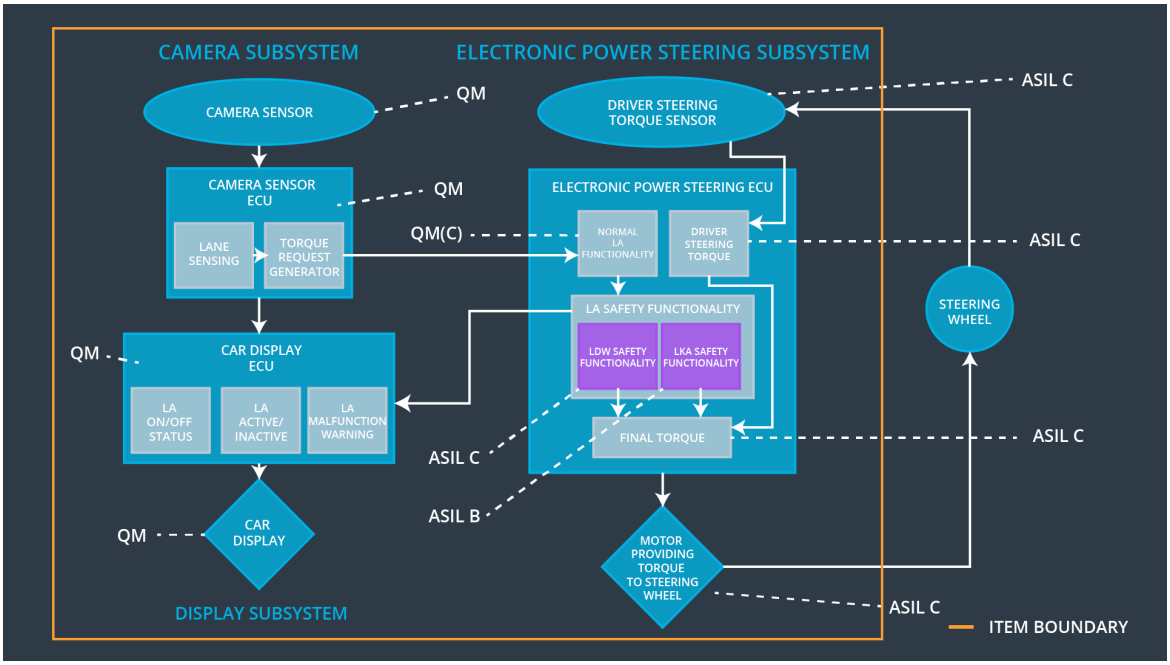
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall shall ensure that the duration of the lane keeping assistance torque applied is less than Max_Duration.	B	500ms	Set the lane keeping add extra torque 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	Validate that the chosen amount for Max_Duration really dissuades drivers from taking their hands off the wheel.	Verify that the system really sets the lane keeping add extra torque to zero if the lane keeping assistance ever exceeds Max_Duration.

Refinement of the System Architecture

The following image shows the refined 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 duration of the lane keeping assistance torque applied is less than Max_Duration.	**X**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn-off LDW functionality	The torque oscillation is above Max_Torque_Amplitude or Max_Torque_Frequency.	Yes, LDW oscillating torque set to zero	Warning Light via car display.
WDC-02	Turn-off LKA functionality	The driver keeps hands off the wheel for longer than Max_Duration	Yes, added LKA torque set to zero.	Warning Light via car display.