Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
08/27/2018	1.0	[NOT_PUBLIC]	Firs submission of the completed functional safety concept
08/28/2018	1.1	[NOT_PUBLIC]	Adapt safe state description

Table of Contents

Purpose of the Functional Safety Concept

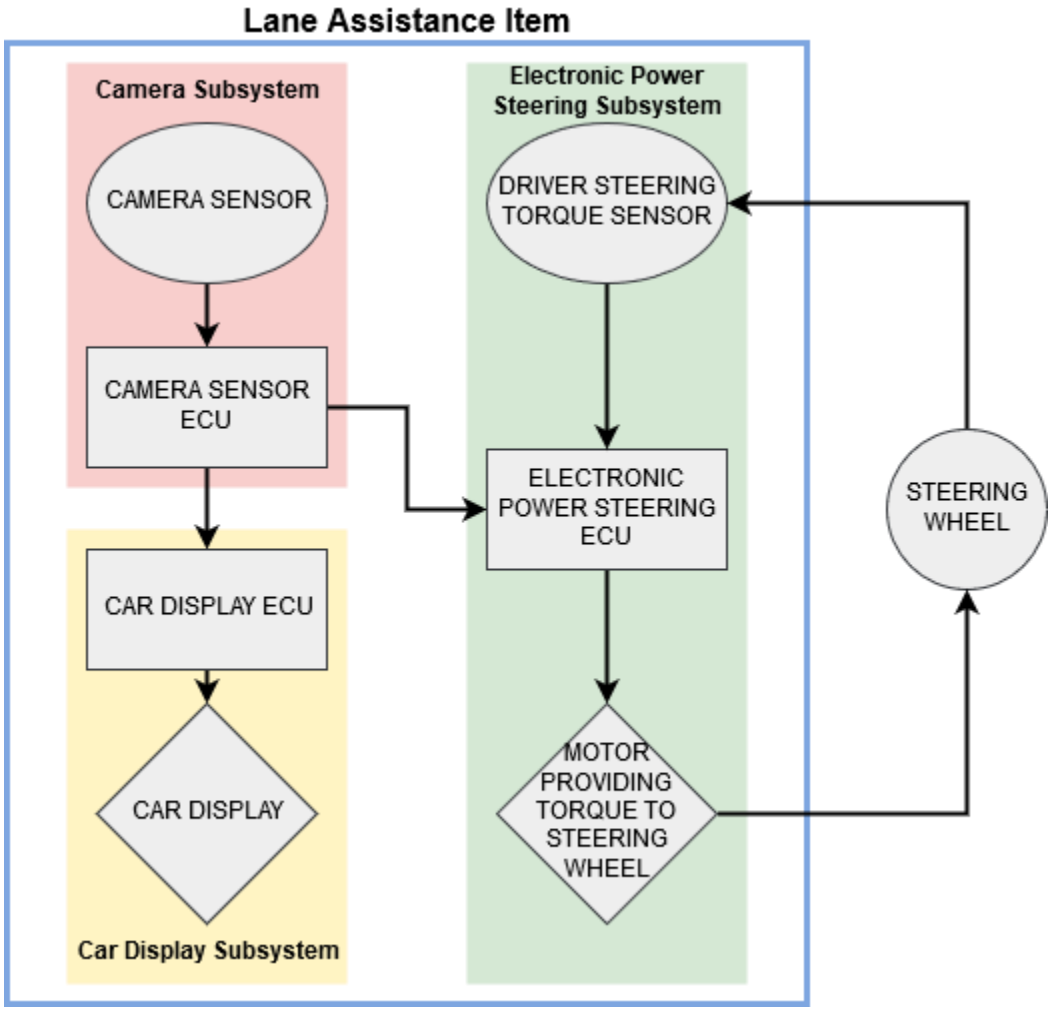
The functional safety concept is looking at the item from a higher level and considers the general functionality. The safety goals derived from the hazard and risk analysis are refined into functional safety requirements and afterwards allocated to their appropriate place in the item architecture. This could involve expanding the system architecture with new elements. Functional safety requirements have a few attributes that need to be specified in the functional safety concept. The functional safety concept also discusses verification and validation, which is how it is proved that the system actually meets the requirements. Later, functional safety requirements are further boiled down to technical safety requirements.

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 LDW 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.
Safety_Goal_03	The lane keeping assistance function shall apply a smaller torque when the wind (lateral force) is in the direction of the applied torque.
Safety_Goal_04	The lane keeping assistance function shall be deactivated when the camera sensor is not able to detect lane lines.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures images and provides them to the Camera Sensor ECU.
Camera Sensor ECU	Detects lane lines, identifies the ego lane (lane the vehicle is in), and calculates the vehicle's distance to the center of the ego lane. Based on that information the Camera Sensor ECU requests a torque to correct the position.
Car Display	Provides visual feedback (warning light) to the driver in the display dashboard.
Car Display ECU	Controls the Car Display and receives information

	about the status of the Lane Assistance System in order to show warning lights accordingly.
Driver Steering Torque Sensor	Senses the torque already applied to the steering wheel by the driver.
Electronic Power Steering ECU	Processes the information received from the Driver Steering Torque Sensor and the torque requested from the Camera Sensor ECU and computes the necessary torque to apply to the steering wheel.
Motor	Applies the torque calculated by the Electronic Power Steering ECU 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)	NO	The lane keeping assistance function is

	function shall apply the steering torque when active in order to stay in ego lane		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 assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Set Final_Torque to zero
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Set Final_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	Test different values of torque amplitude and validate with drivers that the value chosen is high enough to be perceived but low enough to not cause loss of control.	Verify the system sets the Final_Torque to zero in time (50 ms) if Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Test different values of torque frequency and validate with drivers that the value chosen is high enough to be perceived but low enough to not cause loss of control.	Verify the system sets the Final_Torque to zero in time (50 ms) if Max_Torque_Frequency is exceeded.

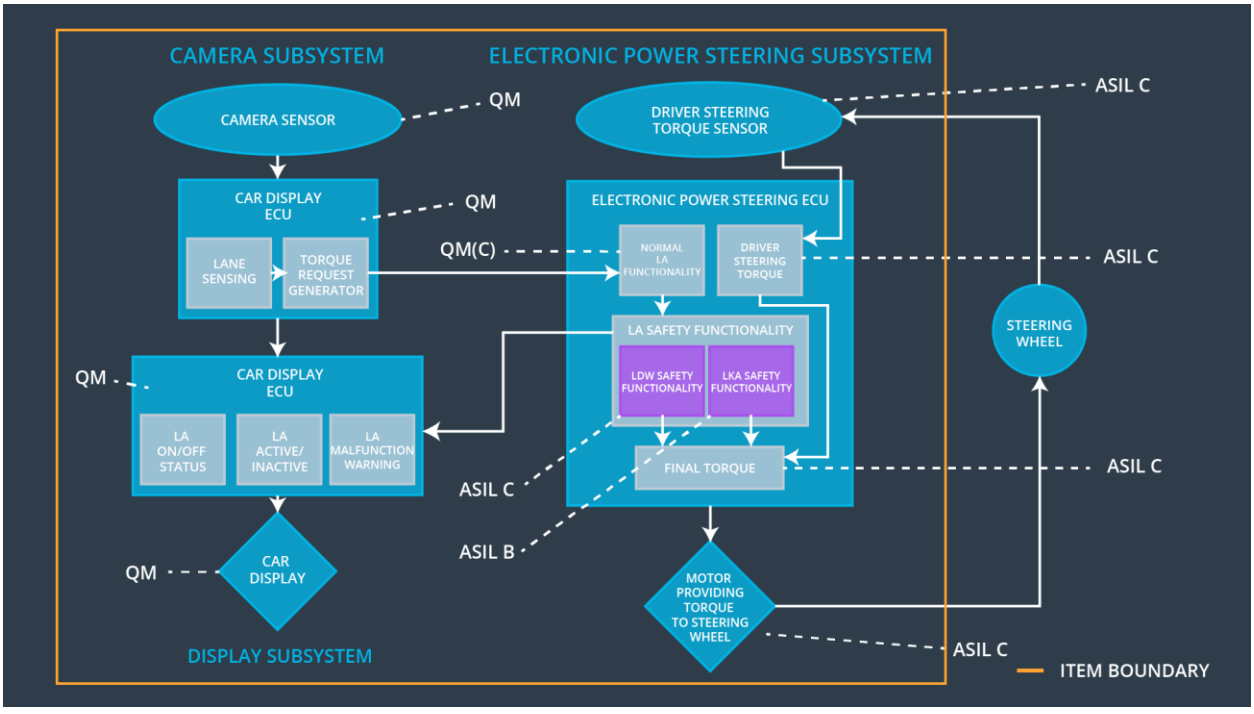
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The lane assistance item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	Set Final_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	Test different valued of max duration and validate with drivers that the value dissuades drivers from taking their hands off the steering wheel.	Verify that the system sets the Final_Torque to zero in time (500 ms) if Max_Duration is exceeded.

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 electronic power steering ECU shall ensure that the lane departure 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 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	Deactivate the system	Malfunction_01 Malfunction_02	Yes	Warning light on display dashboard
WDC-02	Deactivate the system	Malfunction_03	Yes	Warning light on display dashboard