Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2018-09-28	1.0	Rob Poyck	

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept looks at the general high level functionality of the item:

- First it needs to be defined which subsystems contain high levels of risk and what needs to be done to prevent accidents.
- Determine which subsystems and elements can be used to meet safety goals.
- Further refine these goals into functional safety requirements.
- Allocate each functional safety requirement to its appropriate place in the item architecture.
- The subsystems which have new requirements allocated to them might need to be refined, i.e. subdivided and defined in detail.
- Subsystems inherit the ASIL of the requirements and they then might be decomposed to make sure that only the safety critical elements have to be fully analysed according to its higher ASIL level.
- Instructionas are provided on the verification and validation of the requirements.

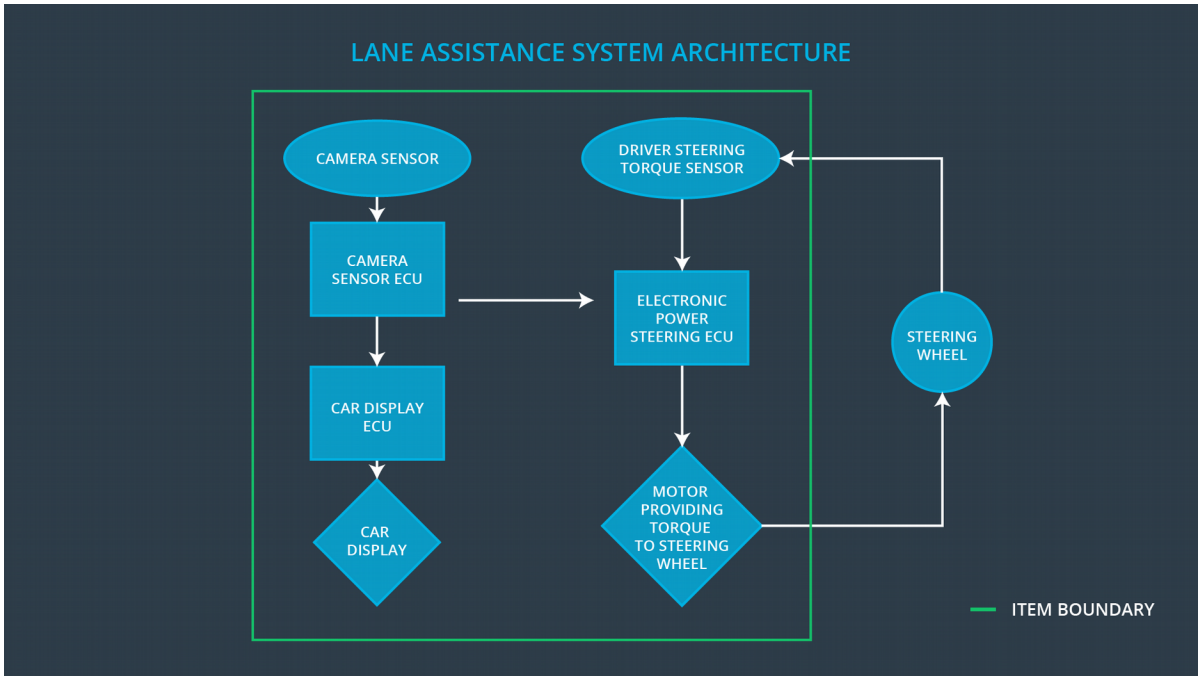
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the 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.
Safety_Goal_03	The torque exerted by the driver shall always be measured correctly within a defined accuracy.

Preliminary Architecture

The preliminary architecture can be seen in the folowing diagram:



Description of architecture elements

Element	Description
Camera Sensor	Provides the camera images for analyses by the camera sensor.
Camera Sensor ECU	Processes the images from the camera sensor in order to determine the position of the vehicle w.r.t. the lane lines. Using this information actuation requests might be sent to the power steering system and the car display when the vehicle leaves the lane unintendedly.
Car Display	Indicate information and warnings/errors to the driver.
Car Display ECU	Processes and stores the requests by the system to show indications and warnings/errors to the driver.
Driver Steering Torque Sensor	Detects the torque already exerted on the steering wheel by the driver.
Electronic Power Steering (EPS) ECU	Takes torque requests from the camera ECU and matches this torque on the steering wheel by requesting the motor to apply the difference between the required torque and the torque already exerted by the driver.
Motor	Applies the torque requested from the EPS 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 oscilating torque applied by the lane departure warning system has a torque amplitude above the defined limit.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The oscilating torque applied by the lane departure warning system has a torque frequency above the defined 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.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the	MORE	The torque exerted by the driver is not

	steering torque when active in order to stay in ego lane (only adding the difference between the required torque and the torque already applied by the driver)		detected and therefore the system overcompensates

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 mas_torque_amplitude.	C	50 [ms]	Lane assistant system turned off.
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below max_torque_frequency.	C	50 [ms]	Lane assistant system turned off.

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 the setting of the maximum torque by gathering the experiences of users with the system to see if the torque amplitude is an an acceptable level.	Verify that the output torque amplitude of the system never exceeds the specified max_torque_amplitude.
Functional Safety Requirement 01-02	Validate the setting of the maximum torque by gathering the experiences of users with the system to see if the torque frequency is an an acceptable level.	Verify that the output torque frequency of the system never exceeds the specified max_torque_frequency.

Lane Keeping Assistance (LKA) Requirements:

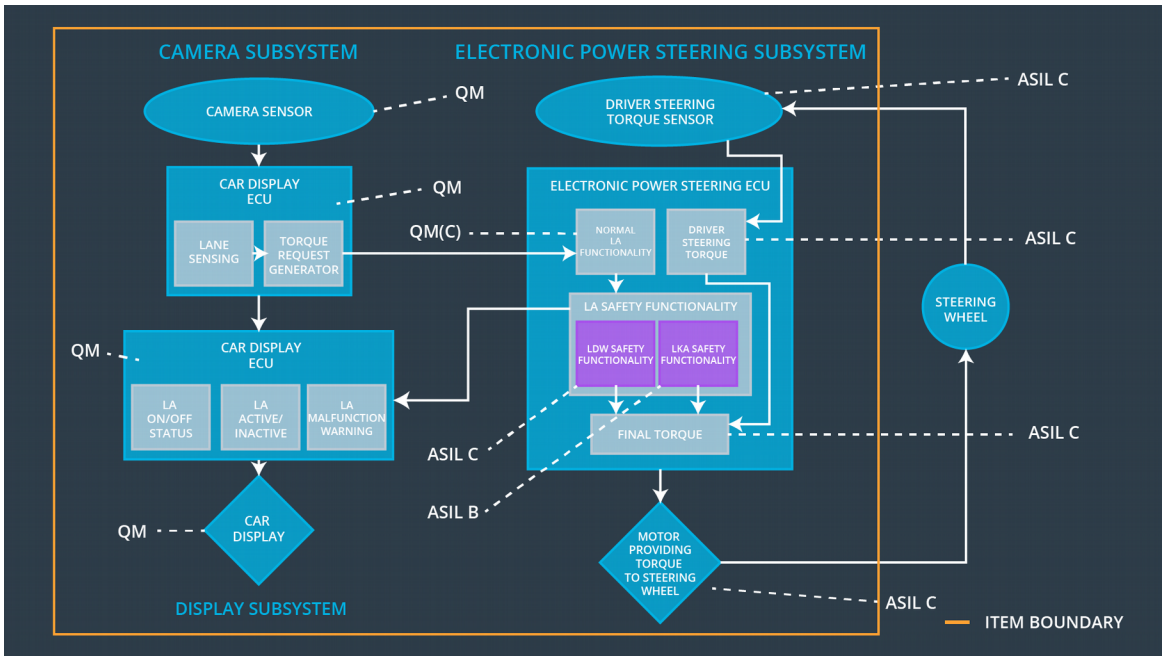
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration.	B	500 [ms]	Lane assistant system turned off.
Functional Safety Requirement 02-02	The system shall only be active when the torque exerted by the driver is propertly detected by the power steering system torque sensor.	D	50 [ms]	Lane assistant system turned off.

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 the setting of the duration by gathering the experiences of users with the system to see if the system is then not misused as an autonomous system.	Verify if the the system is turned off after every operational time of the specified max_duration.
Functional Safety Requirement 02-02	Validate that the system remains active when the normal amount of torque is exerted by the driver, and it turns off when this is not the case.	Verify if the system is indeed automatically turned off when driver torque signals are no longer correctly received.

Refinement of the System Architecture

The refined system architecture, not include the architecture needed satisfy the self-defined additional requirement of making sure that driver input torque is sensed, is shown in the image below.



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 mas_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**		
Functional Safety Requirement 02-02	Validate that the system remains active when the normal amount of torque is exerted by the driver, and it turns off when this is not the case.	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane assistant system turned off.	Malfunction_01, Malfunction_02, Malfunction_03, Malfunction_04	Yes	A lane assistant system malfunction light on the dashboard