



Elektrobit



UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0



Document history

Date	Version	Editor	Description
08/08/2017	1.0	Thomas Ho	Initial version

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

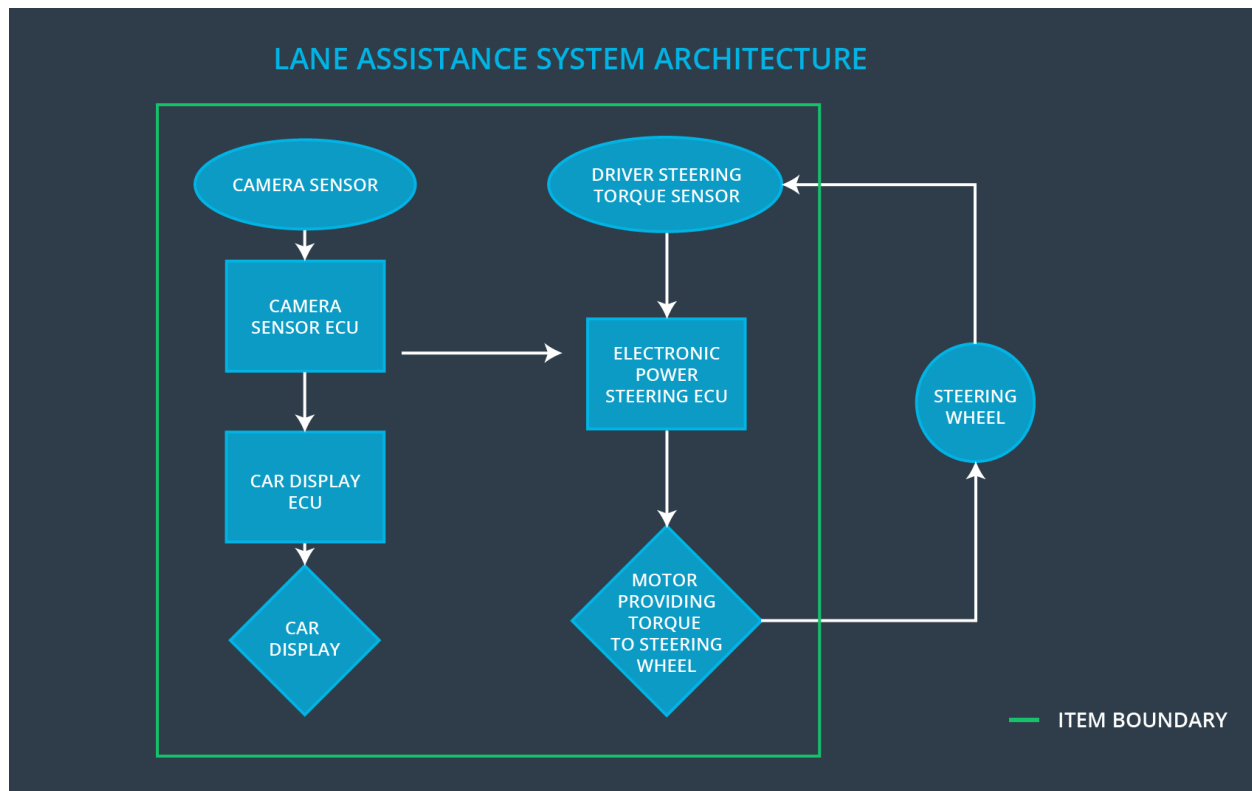
The purpose of functional safety concept is to identify which subsystems and elements can be used to meet safety goals, and allocates functional safety requirements to the relevant parts in the system architecture. Allocation could involve expanding the system architecture with new element blocks.

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 LDW function shall deactivate when the camera sensor is unable to detect road markings, and shall warn the driver of its deactivation.
Safety_Goal_04	The LKA system should check if the Electronic Power Steering ECU is functioning and give warning to driver if it stops working.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Capture and stream images to Camera Sensor ECU for processing
Camera Sensor ECU	Processes image stream from camera sensor to detect lane lines on the road and determine if the vehicle is moving out of the lane unintentionally
Car Display	Graphic interface used to display the warning messages and setting changes.
Car Display ECU	Processes input from camera subsystem and display the messages on the Car Display
Driver Steering Torque Sensor	Responsible for measuring the torque applied by the

	driver.
Electronic Power Steering ECU	Vibrates the steering wheel when vehicle is drifting away from the current lane unintentionally. Add appropriate amount of torque based on feedback from torque sensor to keep vehicle in current lane.
Motor	Actuator used to apply requested torque to 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
Malfunction_04	The LDW function shall deactivate when the camera sensor is unable to detect road markings, and shall warn the driver of its deactivation.	WRONG	The lane keeping warning function is unexpectedly activated and vibrated the steering wheel.
Malfunction_05	The LKA system should check if the Electronic Power Steering ECU is functioning and give warning to driver if it stops working.	WRONG	The lane keep assistance fails to function, but the display shows that it is activated.

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 electronic power steering subsystem shall ensure that the oscillating torque amplitude is less than Max_Torque_Amplitude	C	50 MS	OFF
Functional Safety	The electronic power steering subsystem shall ensure that the oscillating torque	C	50 MS	OFF

Requirement 01-02	frequency is less than 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	Test how drivers react to different torque amplitudes to prove that we chose an appropriate value	Verify that when the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval
Functional Safety Requirement 01-02	Test how drivers react to different torque frequencies to prove that we chose an appropriate value	Verify that when the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval

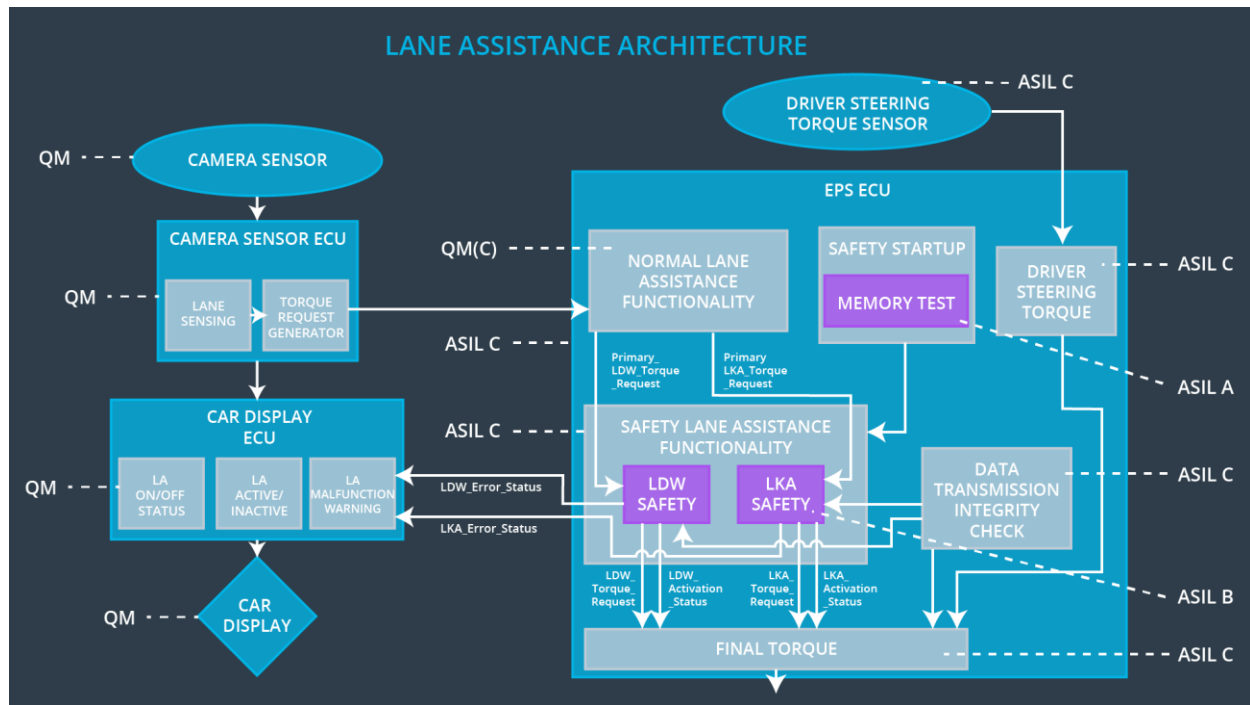
Lane Keeping Assistance (LKA) Requirements:

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	500	OFF

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement	Validate that the Max_Duration chosen really did dissuade drivers from taking	Verify that the system really does turn off if the lane keeping assistance every exceeded MAX_DURATION

Refinement of the System Architecture



The camera sensor ECU has two software blocks:

1. **Lane Sensing** – detect the lane and check if the vehicle is moving away from the ego lane.
2. **Torque Request Generator** – send a torque request to the electronic power steering subsystem

The car display subsystem has three software blocks:

1. **LA ON/OFF Status** – control a light that tells the driver if the lane keeping system on or off.
2. **LA Active/Inactive** – control a light telling the driver that if the lane departure warning is activated.
3. **LA Malfunction Warning** – display warning message if LA system is malfunctioning.

The electronic power steering subsystem has three software blocks:

1. **Normal Lane Assistance Functionality** – receive the vibrational torque request from camera subsystem.
2. **Driver Steering Torque** – sense how much the driver is turning the steering wheel.
3. **Final Torque** – add torque requests together to output a final torque to the motor that move the steering wheel.

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 oscillating torque amplitude is below Max_Torque_Amplitude	x		
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the 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 for only Max_Duration	x		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	OFF	Oscillating torque frequency is higher than Max_Torque_Frequency or torque is higher than Max_Torque_Amplitude	Yes	Car Display
WDC-02	OFF	Lane keeping assistance torque is applied for more than Max_Duration	Yes	Car Display