Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
11/24/17	1.0	Chris Ferone	First draft of document

Table of Contents

Purpose of the Functional Safety Concept

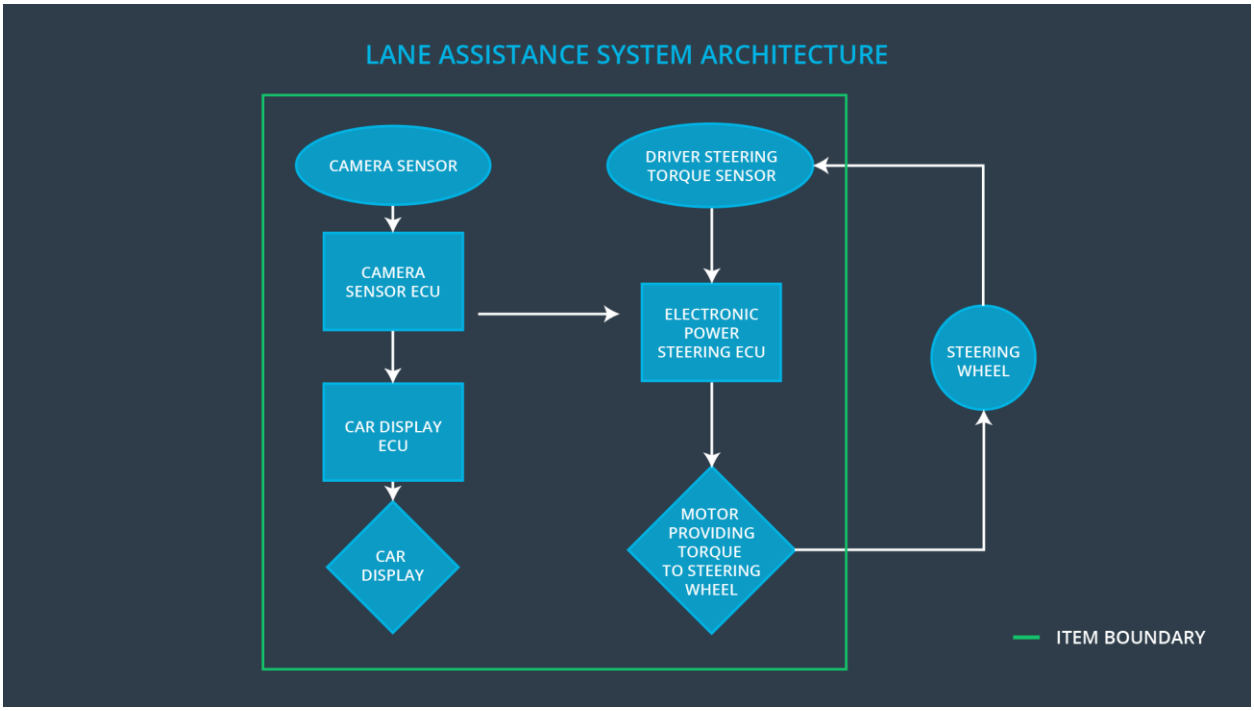
The purpose of the functional safety concept is to refine the safety goals into functional requirements.

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.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures raw image of lane
Camera Sensor ECU	Processes camera data to determine vehicle’s position

	in lane and if a lane departure warning should be issued or if a torque command should be sent to the EPS to keep lane
Car Display	Notifies driver if LDW and LKA are enabled and when they become active
Car Display ECU	Processes information from Camera Sensor ECU and updates Car Display accordingly
Driver Steering Torque Sensor	Measures torque applied to steering wheel by driver
Electronic Power Steering ECU	Controls EPS torque. Listens for torque commands from Camera sensor ECU
Motor	Applies torque to steering column

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	MORE	The lane departure warning function applies an oscillating torque with very high torque frequency

	driver a haptic feedback		(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.

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_Available.	C	50ms	turn off the functionality
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	turn off the functionality

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 a reasonable max torque value was chosen. We would need to 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	validate that a reasonable max	verify that when the torque frequency

Safety Requirement 01-02	frequency value was chosen. We would need to test how drivers react to different frequencies to prove that we chose an appropriate value.	crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

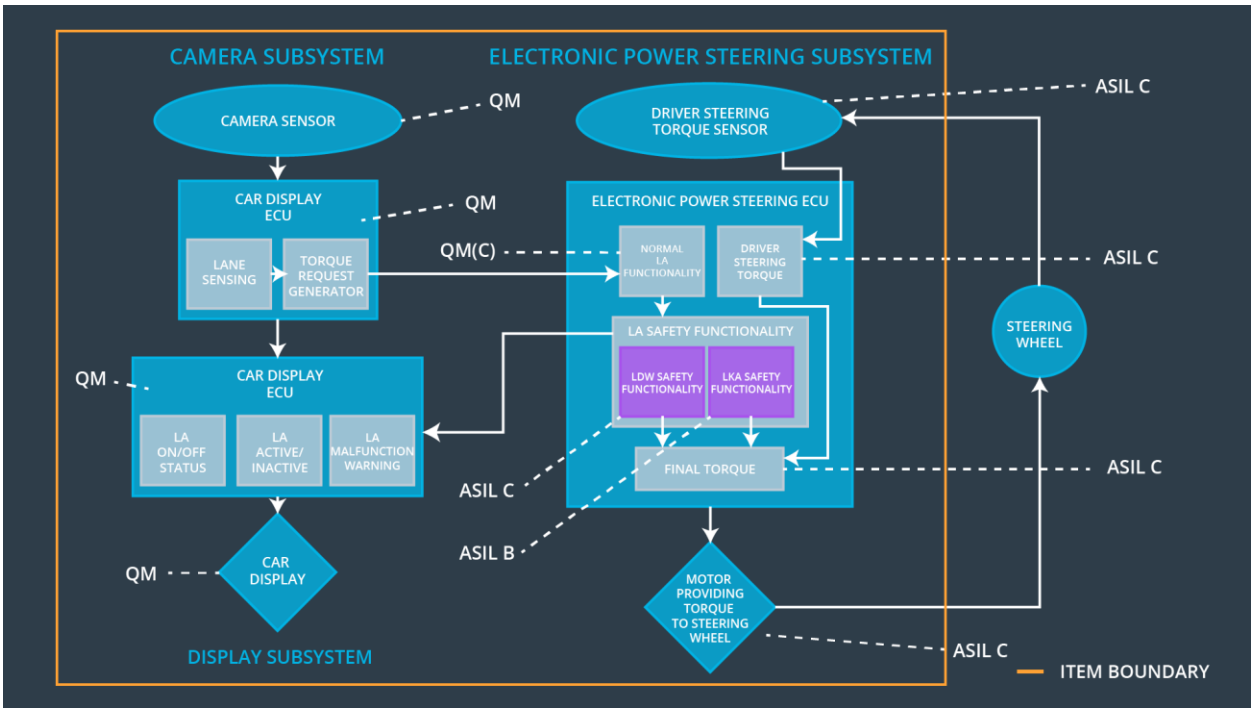
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	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	500ms	turn off the functionality

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 max_duration chosen really did dissuade drivers from taking their hands off the wheel	verify that the system really does turn off if the lane keeping assistance every exceeded 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 electronic power steering ECU shall ensure that the lane departure warning 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 warning oscillating torque amplitude is below Max_Torque_Frequency	**x**		
Functional Safety	the electronic power steering ECU shall ensure that the lane	**x**		

Requirement 02-01	keeping assistance torque is applied for only Max_Duration			

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	turn off the functionality	Malfunction_01, Malfunction_02	Yes	warning light on the dashboard
WDC-02	turn off the functionality	Malfunction_03	Yes	warning light on the dashboard