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
01/09/2018	1.0	Anil Kumar	First version of the document

Table of Contents

Purpose of the Functional Safety Concept

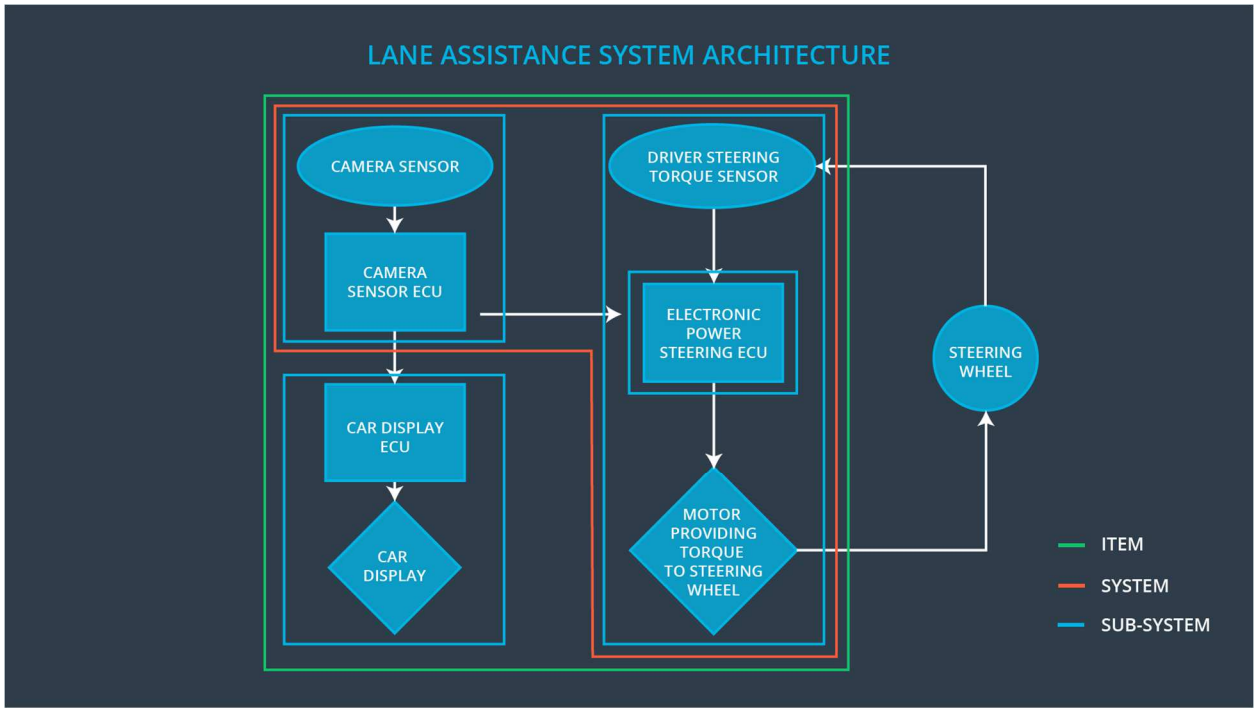
Look at the item from a higher level, identify the new requirements and allocate these requirements to system diagrams

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 the road image stream video
Camera Sensor ECU	the camera system detects lane and lane departure
Car Display	Displays warning and information to the driver
Car Display ECU	Receive commands from other sub systems what and when to be displayed and drives the display according to these commands
Driver Steering Torque Sensor	Senses the torque applied to the steering wheel
Electronic Power Steering ECU	Turns and vibrates the steering wheel according to the request received from Camera Sensor ECU
Motor	Applies torque to the steering wheel according to the value it received from the Camera Sensor ECU

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)	MORE	The lane departure warning function

	function shall apply an oscillating steering torque to provide the driver a haptic feedback		applies an oscillating torque with very high torque amplitude (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 oscillation torque amplitude is below Max_Torque_Amplitude	C	50ms	The oscillation torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillation torque frequency is below Max_Torque_Frequency	C	50ms	The oscillation torque frequency is below 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	max torque amplitude, we chose a reasonable value(low enough to alert the driver and not to cause of steering	When the torque amplitude crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

	wheel)	
Functional Safety Requirement 01-02	max torque frequency, we chose a reasonable value(low enough to alert the driver and not to cause of steering wheel)	When the torque frequency crosses the limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

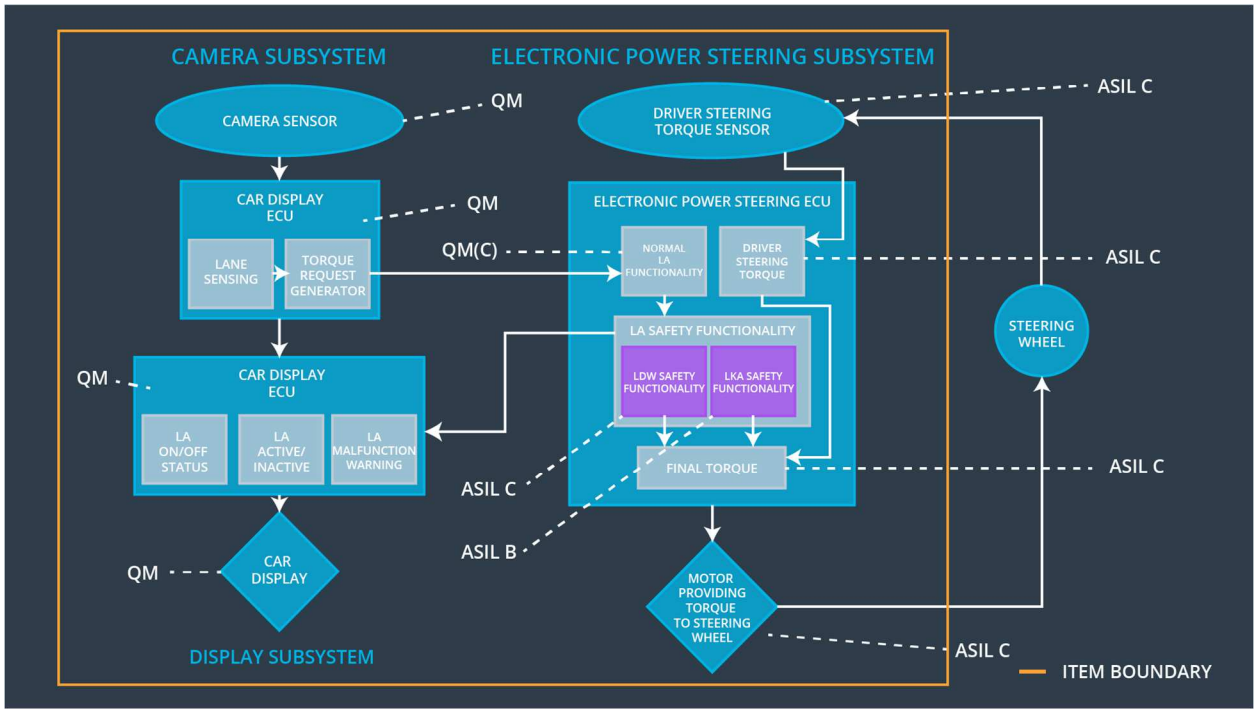
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	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	Lane Keeping Assistance torque set 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	max_duration chosen really did dissuade drivers from taking their hands off the wheel	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 lane keeping item shall ensure that the lane departure oscillation torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillation 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	Turning the system off (The torque request from the lane keeping assistance will be set to zero)	Malfunction_01 Malfunction_02	YES	Turn on Lane Departure warning system malfunction warning light
WDC-02	Turning the system off (The torque request from the lane keeping assistance will be set to zero)	Malfunction_03	YES	Turn on Lane Keep Assis system malfunction warning light