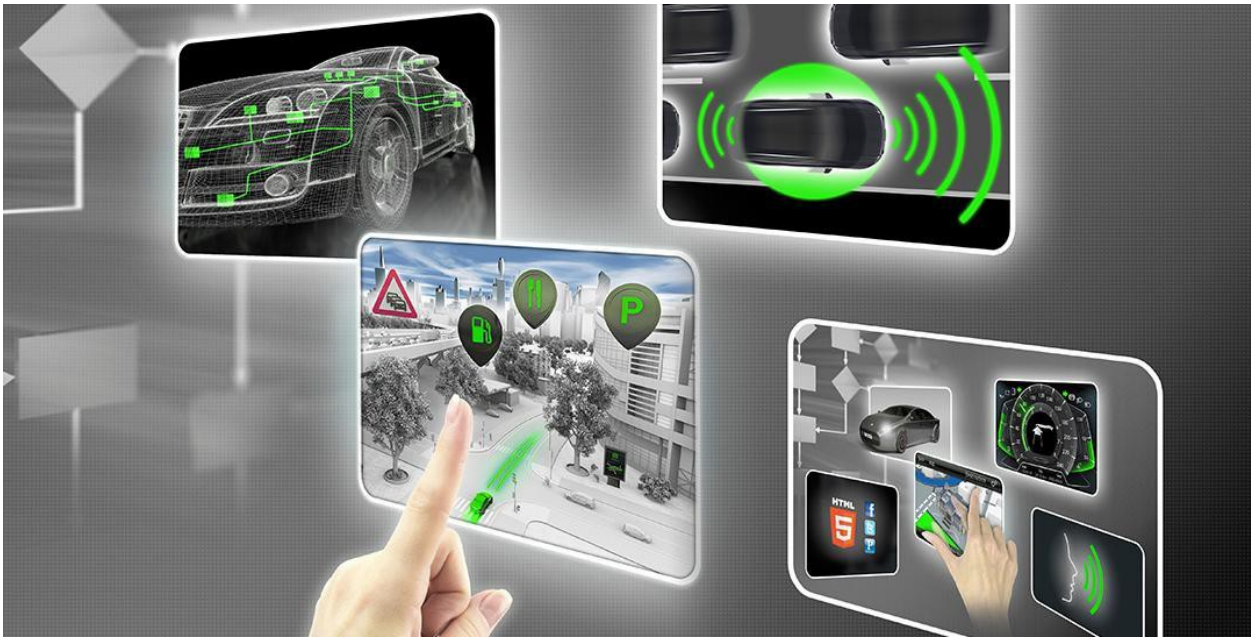
Elektrobit

UDACITY

Functional Safety Concept
Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
27/04/19	1	John Reilly	First Attempt

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept identify new requirements and allocate these requirements to system diagrams. The functional safety concept is looking at the item from a high level.The functional safety concept looks at the general functionality of the item.

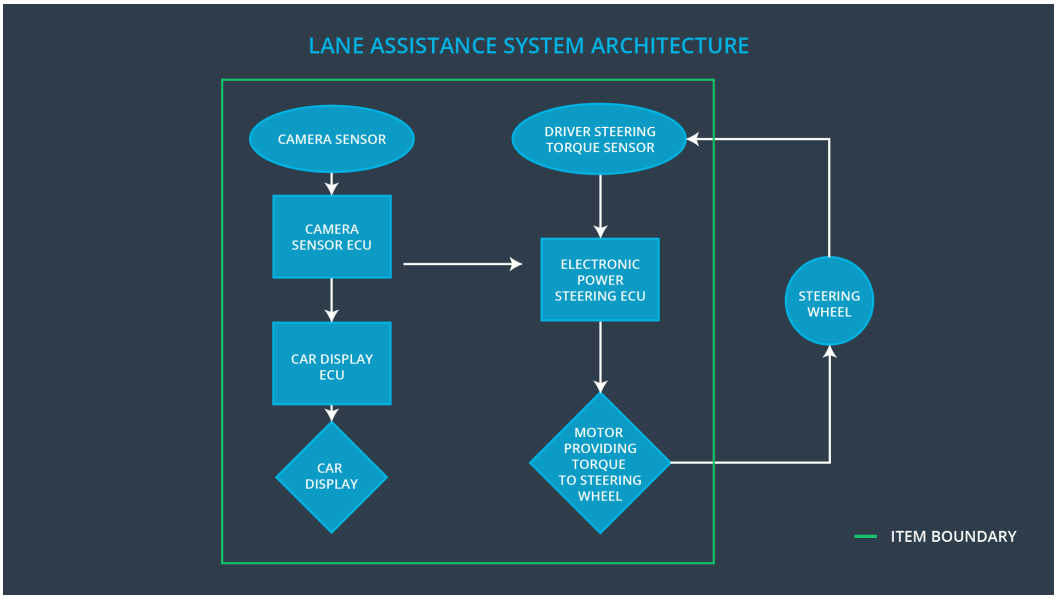
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The the oscilating 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 timer interval so that the driver can not misuse the system for autonomous driving.

Preliminary Architecture

Description of architecture elements



Element	Description
Camera Sensor	Detects optical imformation from the road ahead of the vehicle and send this information to the Camera Sensor ECU
Camera Sensor ECU	Processes information from the camera sensor to detect lanes ahead of the vehicle
Car Display	Displays messages and information about the car to the driver
Car Display ECU	Controls the car display and generates information to be displayed
Driver Steering Torque Sensor	Detects the amount of torque currently being applied to the steering wheel
Electronic Power Steering ECU	Controls the Power Steering subsystem
Motor	Receives control information from the Power Steering ECU and acuates the Steering wheel acordingly

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	MOREThe lane departure warning function applies an oscillating torque with very high torque amplitude (above limit)"	The LDW function applies to high a level of torque in amplitude to the steerring wheelThe 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 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.

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_Amplitude	C	50ms	Oscillating torque amplitude is below Max_Torque_Amplitude
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	Oscillating 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	**Validate** below Max_Torque_Amplitude drivers can easily control vehicle and can still control vehicle at Max_Torque_Amplitude	**Verify** when the torque amplitude crosses the Max_Torque_Amplitude limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.
Functional Safety Requirement	**Validate** below Max_Torque_ Frequency drivers can easily control vehicle and can still control vehicle at	**Verify** when the torque amplitude crosses the Max_Torque_ Frequency limit, the lane assistance output is set

01-02	Max_Torque_ Frequency	to zero within the 50 ms fault tolerant time interval.

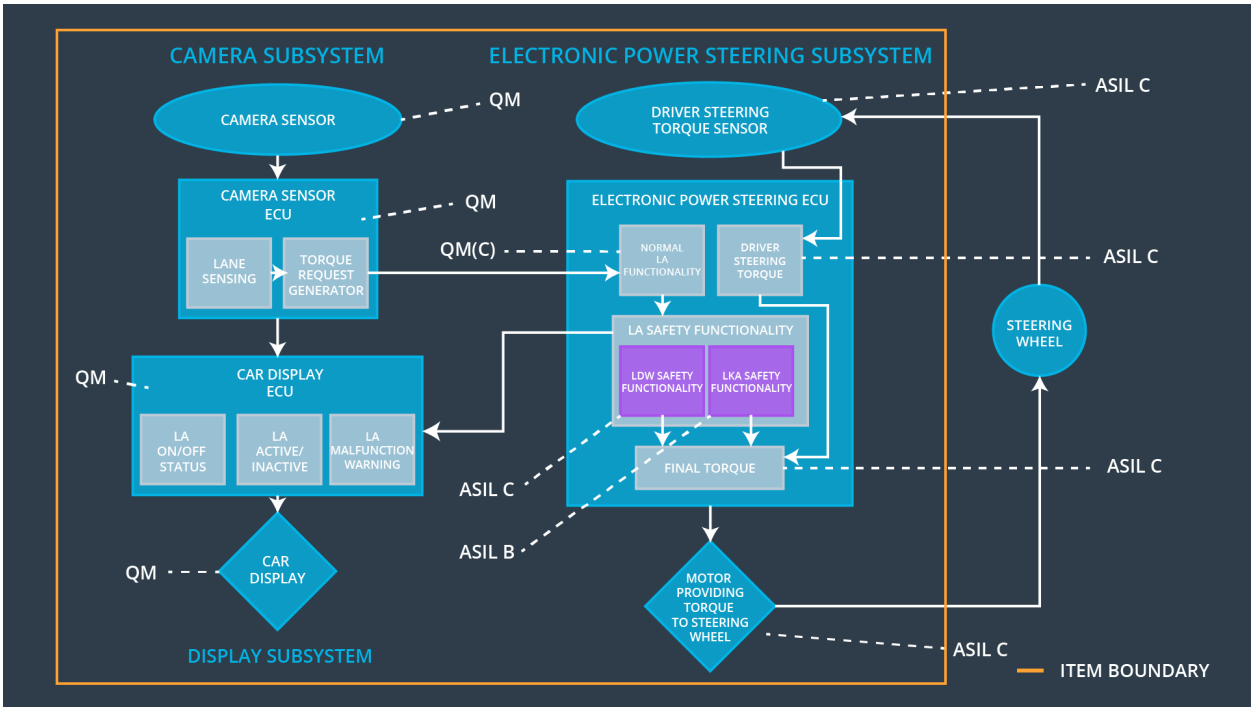
Lane Keeping Assistance (LKA) Requirements:

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 is no longer applied.

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 Max_Duration is short enough to prevent function being used as a self-driving function and long enough to complete function of Lane Keeping	Verify after Max_Duration Lane Keeping Function is disabled.

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 oscillating torque amplitude is below Max_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**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn Off Lane Departure Warning Function	Malfunction_01 Malfunction_02	YES	Dashboard Warning Light/ Warning Message on Display
WDC-02	Turn Off Lane Keeping Function	Malfunction_03	YES	Dashboard Warning Light/ Warning Message on Display