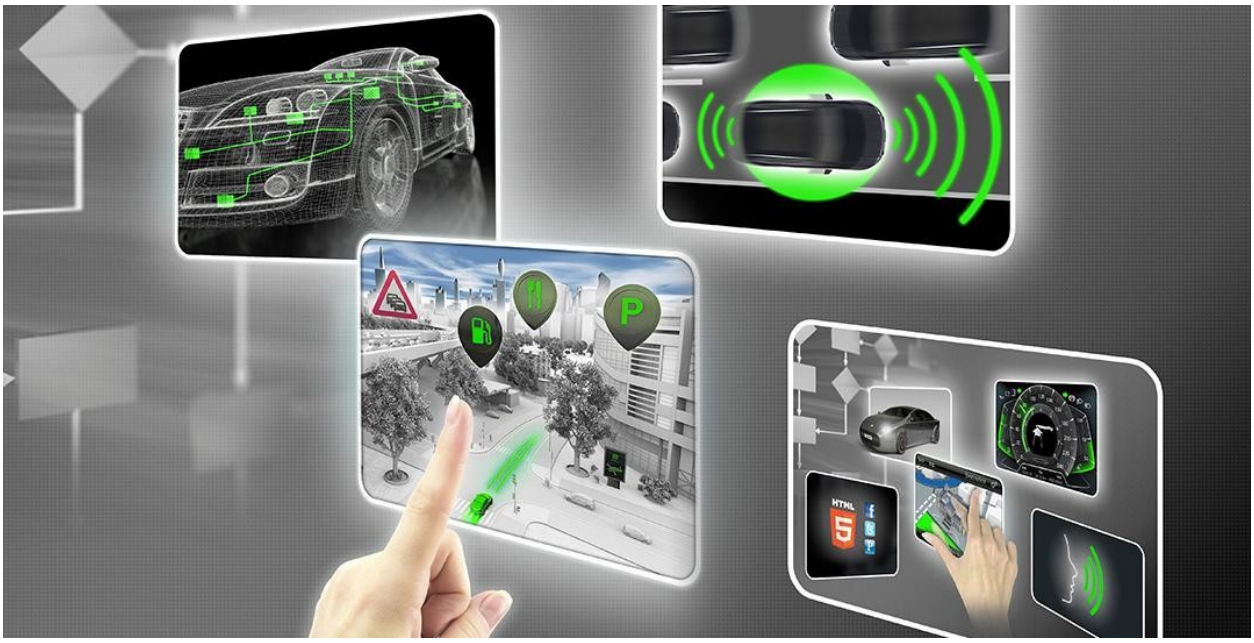
Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
10/9/2018	1.0	John O’Shea	Initial Draft

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

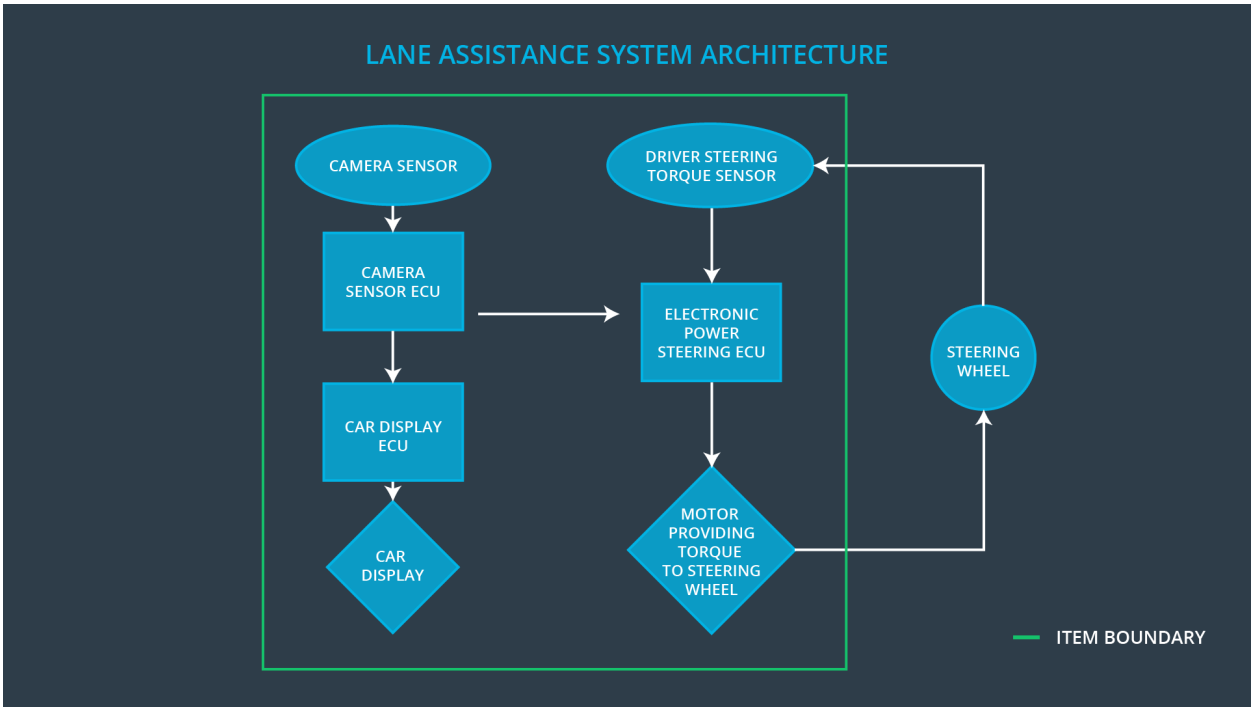
The purpose of the Functional Safety Concept is to performa a system level hazard analysis allocate safety requirements for each hazard. Technical Safety requirements are then derived from the system level safety requirements along with validation and verfication steps for each requirement.

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 (LDW) function shall be limited.
Safety_Goal_02	The Lane Keeping Assistance (LKA) function shall be time limited such that the driver can take over control of the car to help try and avoid a hazard.
Safety_Goal_03	
Safety_Goal_04	

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures images of the road surface and sends them to the Camera Sensor ECU.
Camera Sensor ECU	- Validates the input data (CRC) from the sensor - Processes the image to look for lane lines • Makes a determination of a lane line violation • Alerts Car Display ECU with “Lane Departure Alert” message • Alerts Driver Steering Torque Sensor with “Lane Departure Alert” message
Car Display	Provides a visual indication to the driver if a “Lane Departure Alert ” was detected.
Car Display ECU	• Processes status packets from Camera Sensor ECU. • Detects “Lane Departure Alert” message packet and sets the Car Display warning indicator. • Detects “In Lane” message packet and sets the Car Display by turning off warning indicator
Driver Steering Torque Sensor	Measures the torque applied to the power steering unit.
Electronic Power Steering ECU	• Processes status packets from Drivier Steering Torque Sensor ECU. • Detects “Lane Departure Alert” message packet and sends a command to the motor to apply an oscillating torque to the drive power steering unit. • Detects “In Lane” message packet and send a reset command to disable the oscillating torque if enabled.
Motor	Monitors and applies commands from the Electronic Power Steering ECU to the steering motor.

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 LDW function applies an oscillating torque with very high torque amplitude.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The LDW function applies an oscillating torque with very high torque frequency.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	NO	The LKA function is not limited in time duration.
Malfunction_04			
Malfunction_05			

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 LKA item shall ensure that the lane departure oscillating torque is below Max_Torque_Amplitude.	C	50 ms	The torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The LKA item shall ensure that the lane departure oscillating torque is below Max_Torque_Frequency.	C	50 ms	The 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	Apply LDW tests to validate the Max_Torque_Amplitude is high enough to alert the driver, but below an uncomfortable level that might cause loss of control.	Verify that the torque applied by the power steering ECU is disabled (0Nm) if the Max_Torque_Amplitude is exceeded.
Functional Safety Requirement 01-02	Apply LDW tests to validate the Max_Torque_Frequency is high enough to alert the driver, but below an uncomfortable level that might cause loss of control.	Verify that the torque applied by the power steering ECU is disabled (0Nm) if the Max_Torque_Frequency is exceeded.
Functional Safety Requirement 01-03		

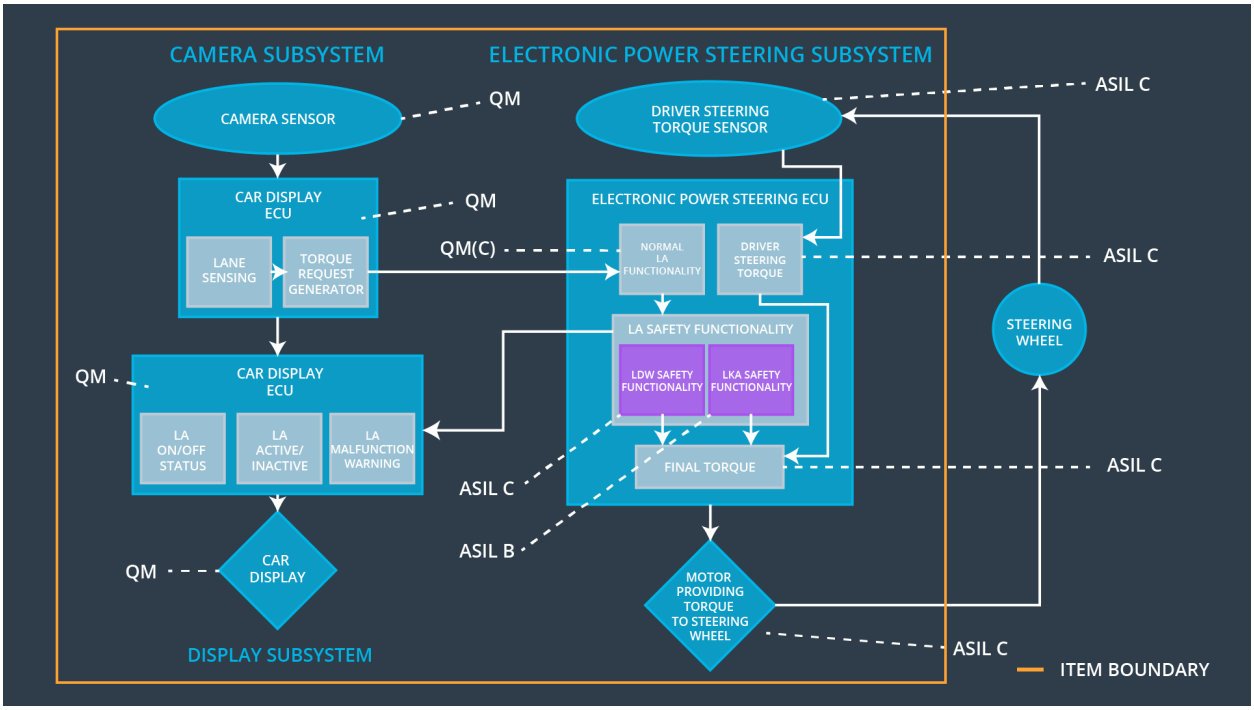
Lane Keeping Assistance (LKA) Requirements:

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 torque is applied only for Max_Duration.	B	500 ms	The torque applied by the power steering ECU after Max_Duration is 0Nm.

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 Max_Duration is long enough to alert the driver to take contol of the steering wheel	Verify that the LKA is disabled when Max_Duration is reached.
Functional Safety Requirement 02-02		

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 LKA shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**X**		
Functional Safety Requirement 01-02	The LKA shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	**X**		
Functional Safety Requirement 01-03				
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the LKA torque is applied for Max_Duration.	**X**		
Functional Safety Requirement 02-02				

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW is disabled	Malfunction_01, Malfunction_02,	Yes	Car Display provides visual indication that LDW is disabled
WDC-02	LKA is disabled	Malfunction_03	Yes	Car Display provides visual indication that LKA is disabled