Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
22/05/2018	1.0	Ashith Raghunath	Compiled functional safety concept

Table of Contents

Purpose of the Functional Safety Concept

The ultimate goal of functional safety is to avoiding accidents by reducing risk to acceptable levels. In order to achieve this, we document the following attributes into a document called the Functional Safety Concept:

- Looking at the items architecture we first identify which all subsystems and elements can be used to meet the safety goals
- Then we further refine the safety goals into what are called safety requirements.
- Then we allocate the safety requirements into its appropriate place in the item architecture.
- We then refine the system architecture to handle the new requirements

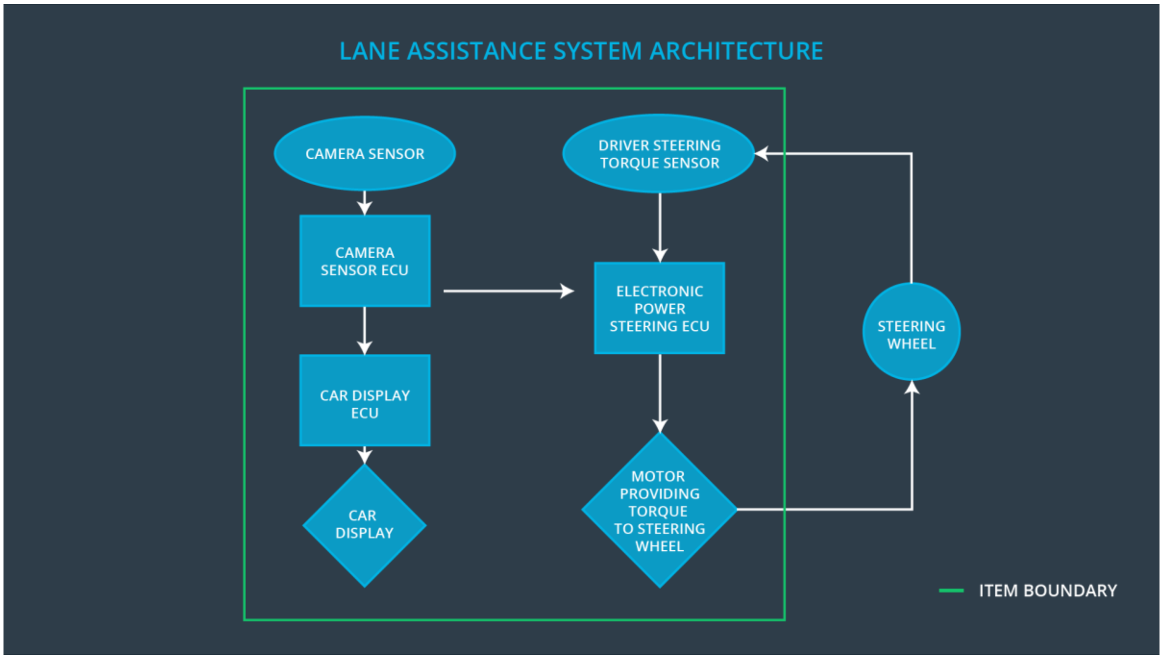
Inputs to the Functional Safety Concept

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 additional steering torque shall end after a given time interval so the driver cannot misuse the system for autonomous driving.

Preliminary Architecture

Below is a preliminary architecture for the lane assistance item.


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Description of architecture elements

Element	Description
Camera Sensor	It is used to capture the images of the road ahead and pass it on to the Camera Sensor ECU
Camera Sensor ECU	Use OpenCV methods to analyze the input images and Localize the car with respect to the lane lines. It then calculates the torque necessary to center the vehicle in the lane.
Car Display	Provide visual display for warnings related to any of the functions such as lane departure warning.
Car Display ECU	Takes input from the Camera Sensor ECU and drive the Display to show the appropriate warnings.
Driver Steering Torque Sensor	Measures the amount of torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	It takes the torque necessary to center the car and the torque already applied by the driver and calculates the

	additional torque that is to be applied by the Motor
Motor	Applies the required torque received from the Electronic Power Steering ECU to the 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

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 max amplitude is below Max_Torque_Amplitude	C	50ms	Limit the torque below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque max frequency is below Max_Torque_Frequency	C	50ms	Limit the torque 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	The Max_Torque_Amplitude should be set to resonable value that can be handled by the driver as well as ensure he can detect it.	Verify that 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 01-02	The Max_Torque_ Frequency should be set to resonable value that can be handled by the driver as well as ensure he can detect it.	Verify that when the torque amplitude crosses the Max_Torque_ Frequency limit, the lane assistance output is set to zero within the 50 ms fault tolerant time interval.

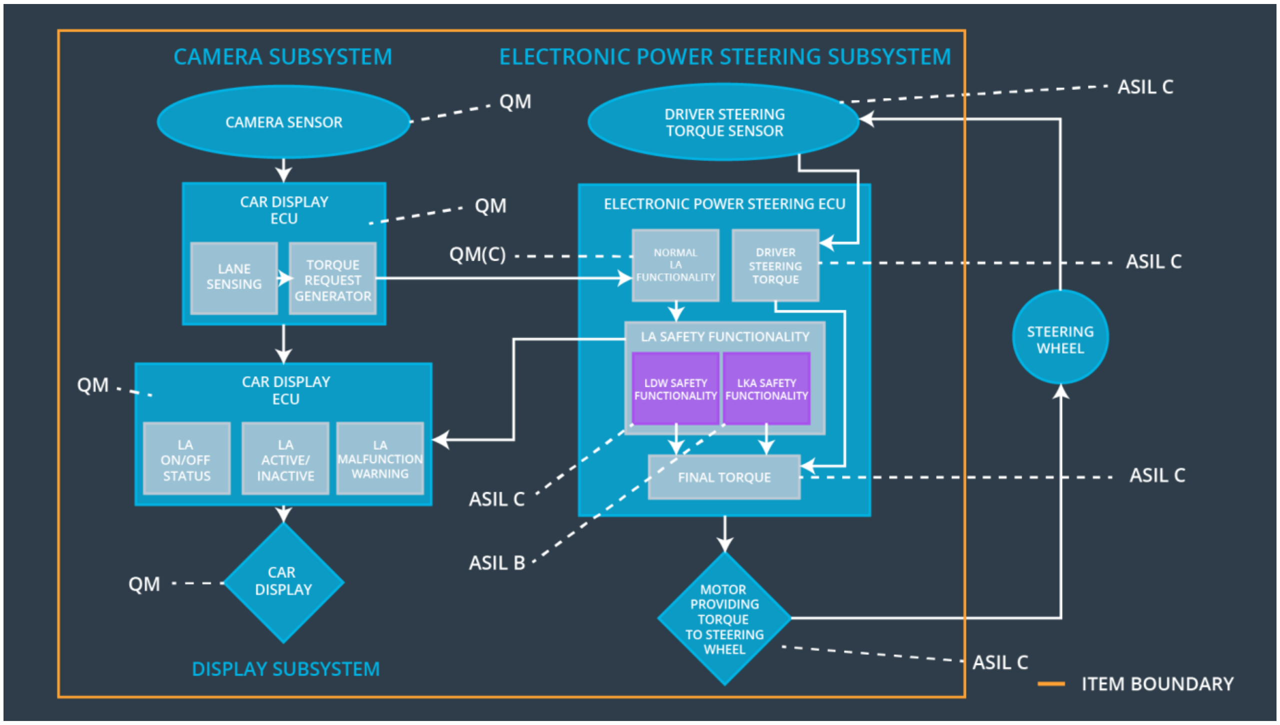
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	lane keeping assistance function shall be time limited and the additional steering torque shall end after a given timer interval (MAX_DURATION)so that the driver cannot misuse the system for autonomous driving	B	500ms	Turn off the lane keeping assistance function

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 should be set to an appropriate value that 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 oscillating torque max amplitude is below Max_Torque_Amplitude	x		
Functional Safety Requirement 01-02	The Electronic Power Steering ECU shall ensure that the lane departure oscillating torque max 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 the functionality	Malfunction_01 Malfunction_02	Yes	Display a Lane Departure Warning Malfunction warning on Car Display
WDC-02	Turn off the functionality	Malfunction_03	Yes	Display a Lane Keeping Assistance Malfunction warning on Car Display