Functional Safety Concept Lane Assistance

Document Version: 1.0, Released 2018-07-01

Document history

Date	Version	Editor	Description
07/01/2018	1.0	Anand Mandapati	Initial version

Table of Contents

# Purpose of the Functional Safety Concept

The purpose of the Functional Safety Concept portion of the Safety Plan is to derive general hardware and software requirements that mitigate the identified risks in the electrical and electronic components that constitute the Lane Assistance System. The requirements are then allocated to the appropriate location in the system architecture. This could involve expanding the system architecture with new element blocks, if necessary.

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
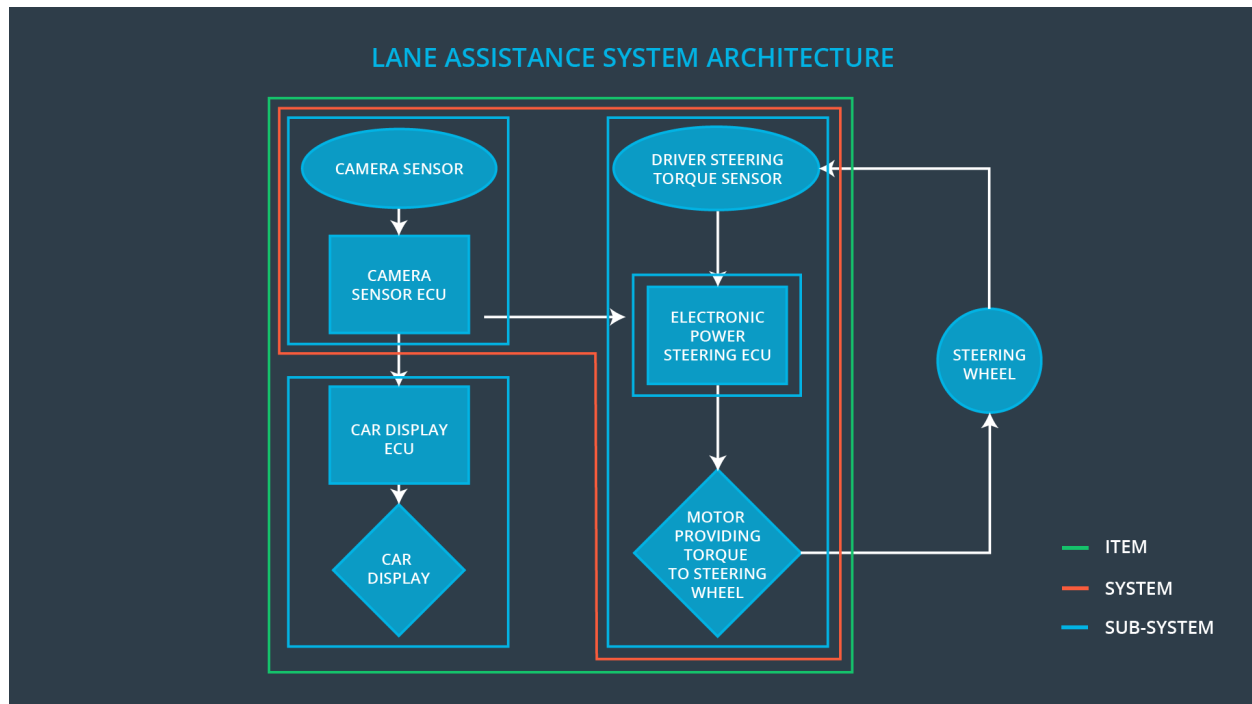
Description of architecture elements

Element	Description
Camera Sensor	Senses images of the road ahead of the vehicle.
Camera Sensor ECU	Detects lane lines on the images, derives position and direction of vehicle relative to the lane and generates torque request.
Car Display	Informs the driver about the state of the vehicle, including status and warnings of the LDW & LKA functions.
Car Display ECU	Process information for display to the driver.
Driver Steering Torque Sensor	Senses steering torque provided manually by the driver.
Electronic Power Steering ECU	Implements the logic behind both Lane Assistance System functions. Processes the inputs from the Camera Sensor ECU and Driver Steering Torque Sensor and controls the Motor that provides torque to the steering wheel.
Motor	Proivides torque 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 oscillation torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Reduce oscillating steering torque to zero
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillation torque frequency is below Max_Torque_Frequency.	C	50 ms	Reduce oscillating steering torque to zero

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 Max_Torque_Amplitude is chosen high enough that the driver notices it but low enough not to cause loss of steering.	Verify that the system really sets oscillating torque to zero if the lane departure warning ever causes a vibration above Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate that Max_Torque_Frequency is chosen high enough that the driver notices it but low enough not to cause loss of steering.	Verify that the system really sets oscillating torque to zero if the lane departure warning ever causes a vibration above Max_Torque_Frequency.

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	500 ms	Reduce augmented steering torque 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	Validate that the chosen amount for Max_Duration really dissuades drivers from taking their hands off the wheel.	Verify that the system really sets the extra torque to zero if the Lane Keeping Assistance ever exceeds Max_Duration.

Refinement of the System Architecture
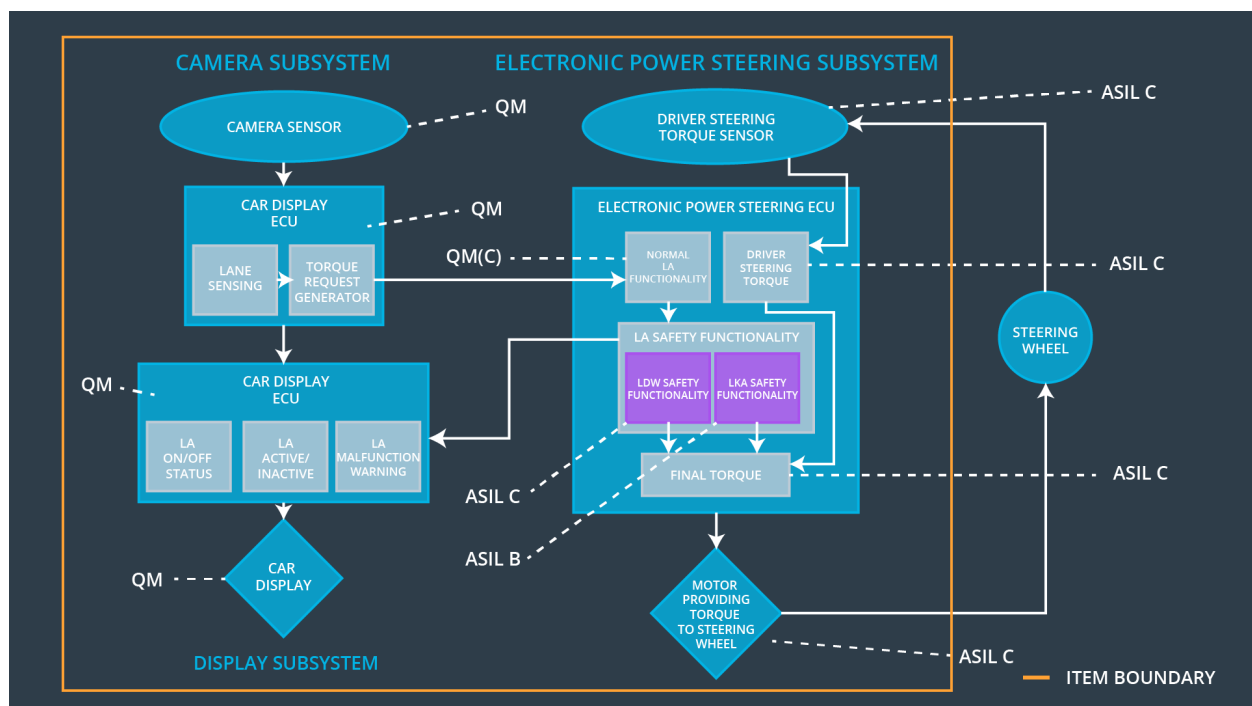
Allocation of Functional Safety Requirements to Architecture Elements

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 oscillation torque amplitude is below Max_Torque_Amplitude.	x		
Functional Safety Requirement 01-02	The Electronic Power Steering ECU 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	Turn-off LDW function	The torque oscillation is above Max_Torque_Amplitude or Max_Torque_Frequency.	Yes, oscillating sttering torque reduced to zero	Warning on Car Display.
WDC-02	Turn-off LKA function	The driver keeps hands off the wheel for longer than Max_Duration	Yes, augmented steering torque set to zero.	Warning on Car Display.