Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

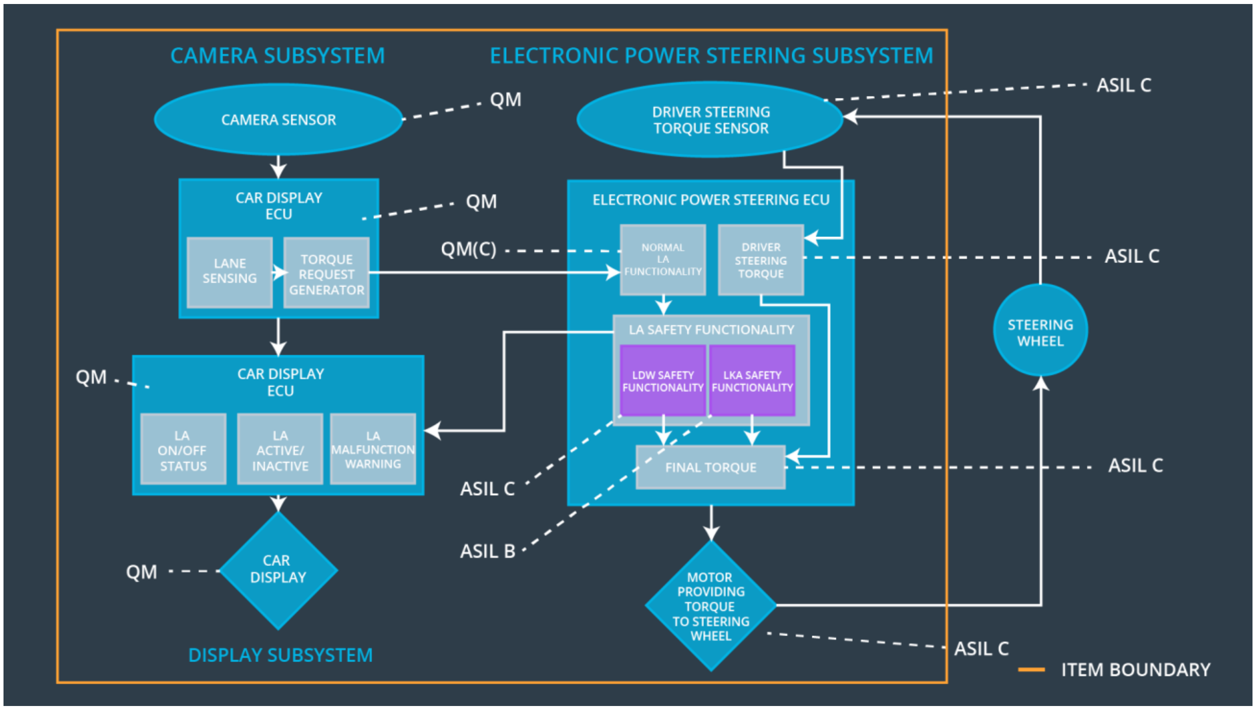
[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
23/05/2018	1	Arpit Srivastava	First attempt

Table of Contents

[Instructions: We have provided a table of contents. If you change the document structure, please update the table of contents accordingly. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]



Allocation of Functional Safety Requirements to Architecture Elements

Warning and Degradation Concept

Purpose of the Functional Safety Concept

The high level requirements are identified and each item is allocated with certain requirements. To determine the requirements for technical safety these concepts are used. These concepts are followed by validation and verification procedure.

Inputs to the Functional Safety Concept

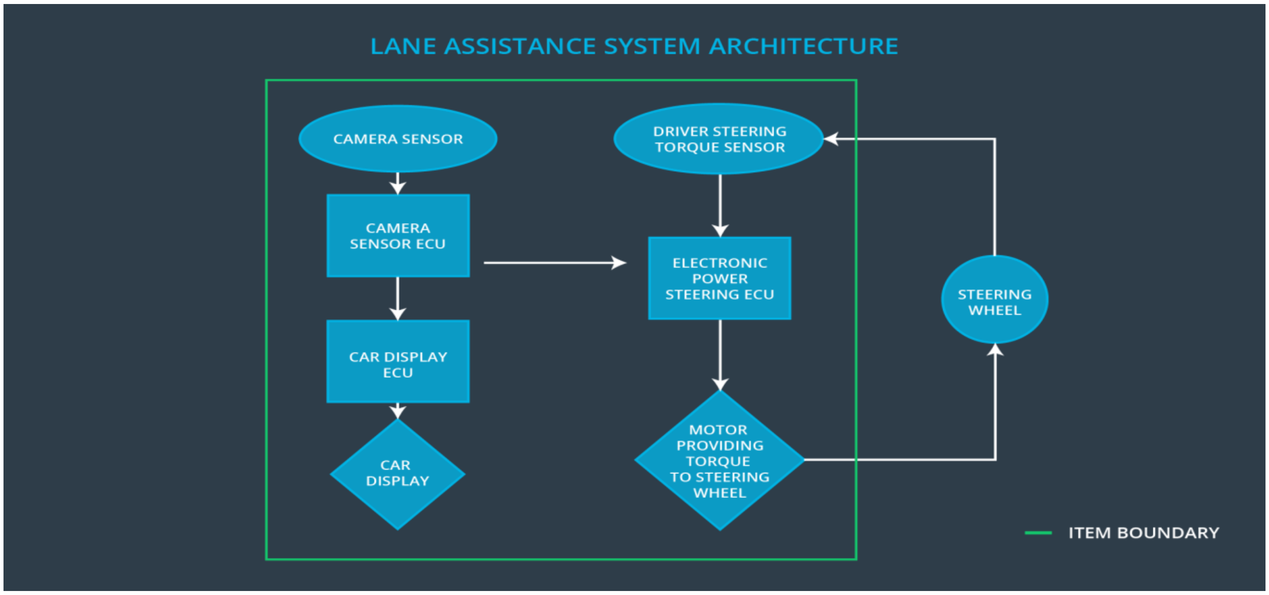
Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the Lane Departure Warning function shall be capped.
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.
Safety_Goal_03	Customized warning for snowy conditions.

Safety_Goal_04	Warning system onboard for malfunctioning camera assist

Preliminary Architecture

The architecture for lane assistance is as follows:


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	Capture the video feed of the road and provide as image frames.
Camera Sensor ECU	Responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
Car Display	Display warning, feedback, messages and lane assistance information to the driver.
Car Display ECU	Drive the Car Display component to show the Lane Keeping Assistance warning and Lane Departure Assistance status.
Driver Steering Torque Sensor	Measure the torque applied to the steering wheel by the driver.
Electronic Power Steering ECU	The component calculates the remaining torque required by taking note of the torque applied by driver (received from sensor) and the torque suggested by

	lane assistance.
Motor	Applies the torque indicated by 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

[Instructions: Fill in the functional safety analysis table below.]

Malfunction ID	**Main Function of the Item Related to Safety Goal Violations**	**Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)**	**Resulting Malfunction**
Malfunction_01	The oscillating steering torque from the Lane Departure Warning function shall be capped.	MORE	The Lane Departure Warning function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction_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.	MORE	The Lane Keeping Assistance function is not limited in time duration which lead to misuse as an autonomous driving function.
Malfunction_03	Customized warning for snowy conditions.	NO	The Lane Keeping Assistance function is limited by adverse environmental conditions.

Malfunction_04	Warning system onboard for malfunctioning camera assist	LATE	The lane keeping assistance is faulty.

Functional Safety Requirements

[Instructions: Fill in the functional safety requirements for the lane departure warning]

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Vibration torque amplitude below Max_Torque_Amplitude.
Functional Safety Requirement 01-02	The Lane Departure Warning item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	B	50 ms	Vibration 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 Max_Torque_Amplitude chosen is high enough to be detected by a driver while low enough not to cause loss of steering	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Amplitude.
Functional Safety Requirement 01-02	Validate Max_Torque_Frequency chosen is adequate to be detected by the driver and not cause the loss of steering.	Verify the system does turn off if the Lane Departure Warning exceeded Max_Torque_Frequency.

[Instructions: Fill in the functional safety requirements for the lane keeping assistance]

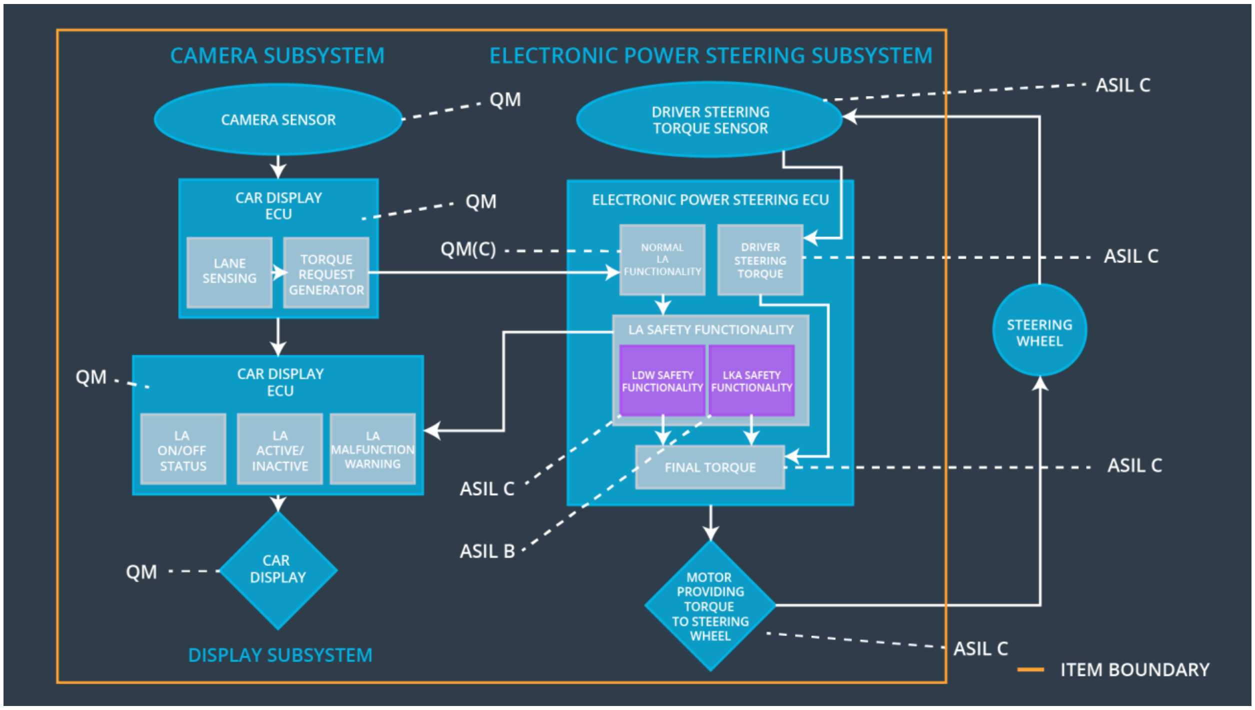
Lane Keeping Assistance (LKA) Requirements:

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 only Max_Duration.	B	300 ms	Lane Keeping Assistance torque is zero.
Functional Safety Requirement 02-02	It will be ensured that the camera is not faulty.	C	50 ms	Lane Keeping Assistance camera is working properly.

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 chosen not allow the driver to use the car as self-driving car.	Verify the system does deactivate if the Lane Keeping Assistance torque application exceeded Max_Duration.
Functional Safety Requirement 02-02	Validate that the camera is not faulty and gives a lag free feedback.	The results are validated in realtime.

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

[Instructions: Mark which element or elements are responsible for meeting the functional safety requirement. Hint: Only one ECU is responsible for meeting all of the requirements.]

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-01	The Lane Departure Warning item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	X		
Functional Safety Requirement 01-02	The Lane Departure Warning 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 only Max_Duration.	**X**		
Functional Safety Requirement 02-02	It will be ensured that the camera is not faulty.		**X**	

Warning and Degradation Concept

ID	**Degradation Mode**	**Trigger for Degradation Mode**	**Safe State invoked?**	**Driver Warning**
WDC-01	Turn off Lane Departure Warning functionality	Malfunction_01, Malfunction_04	Yes	Lane Departure Warning Malfunction Warning on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality	Malfunction_02, Malfunction_03	Yes	Lane Keeping Assistance Malfunction Warning on Car Display