Functional Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
18/08/2018	1.0	Jumana MP	First Attempt

Table of Contents

Purpose of the Functional Safety Concept

Functional safety concept documents the high-level system safety requirements from the general functionality of the item. The identified requirements are then attributed to the various parts of the item architecture. Initially, the requirements are identified based on safety goals identified in the hazard and risk analysis process. During the preparation of functional safety concept, new requirements are identified and allocated which leads to redefining the item architecture. For every part of the architecture that has a safety requirement, corresponding ASIL level is represented. During this process, decomposition of ASIL levels are performed to deal with multiple ASIL level occurring on same component as well as to make sure that the ASIL is maximum avoided from non-safety critical software. The document also covers how to verify and validate the requirements captured. Moreover, warning and degradation mechanisms for every requirement is documented.

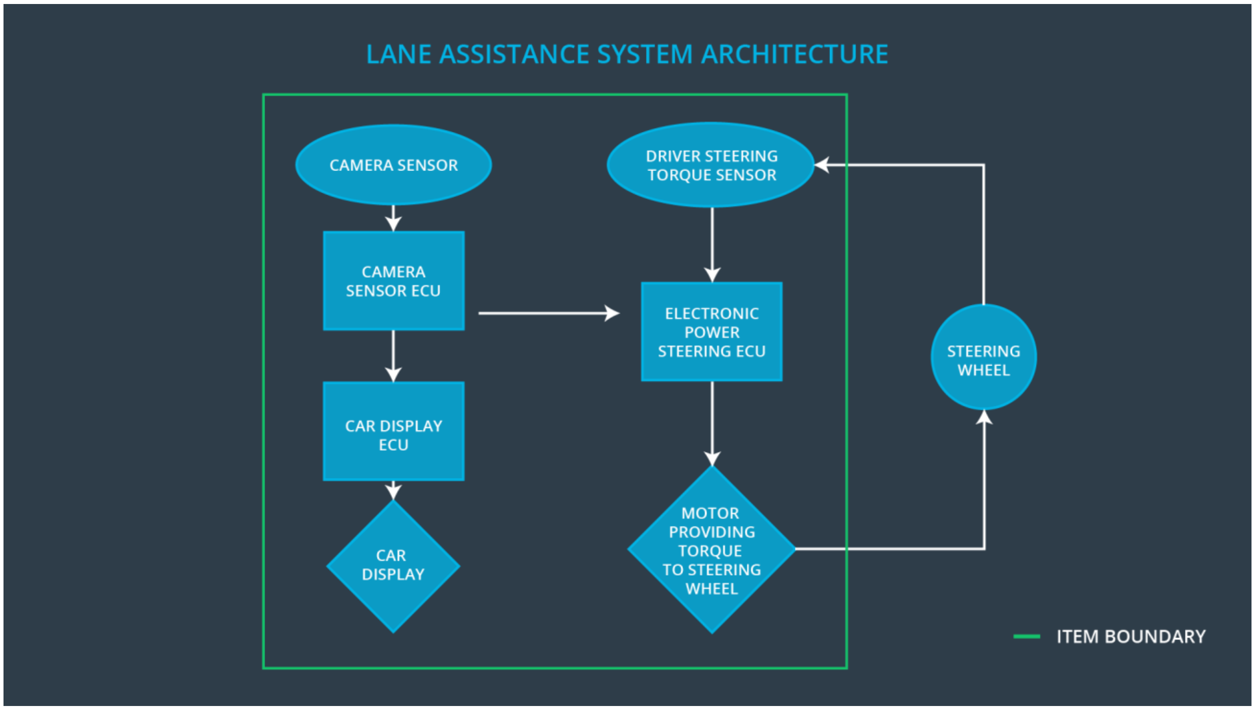
Inputs to the Functional Safety Concept

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.
Safety_Goal_03	The lane detection shall not be activated if camera sensor is failing due to bad weather conditions like snow.
Safety_Goal_04	The lane detection shall take wind force into account for torque calculation.

Preliminary Architecture

Figure below shows the preliminary system 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	Captures images from the road.
Camera Sensor ECU	Identifies when the ego car has departed out of the lane accidentally and sends the signals to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	Informs driver about the warnings and status from the Lane Assistance system.
Car Display ECU	Drives the Car Display component by providing it with the warning and status data.
Driver Steering Torque Sensor	Measures the torque value to the steering wheel provided by the driver.
Electronic Power Steering ECU	Captures the torque information from the Driver Steering Torque Sensor and the camera sensor data that gives information about the lane departure to provide the necessary torque to be applied to the steering wheel motor actuator.
Motor	Applies the torque provided 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

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)	MORE	The lane departure warning function applies

	function shall apply an oscillating steering torque to provide the driver a haptic feedback		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
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The lane departure warning function applies a sudden oscillating torque falsely due to wrong detections by camera sensor failure due to snow.
Malfunction_05	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	LESS	The lane departure warning function applies an oscillating torque which is less for the car to be in lane as there is lateral wind in opposite direction.

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 assistance item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	C	50ms	Deactivate the function
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Deactivate the function

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 the value chosen for Max_Torque_Amplitude is reasonable by testing how different drivers react to various values.	Verify that the entire system turns off if the torque amplitude ever exceeds the Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate the value chosen for Max_Torque_Frequency is reasonable by testing how different drivers react to various values.	Verify that the entire system turns off if the torque frequency ever exceeds the Max_Torque_Frequency

Lane Keeping Assistance (LKA) Requirements:

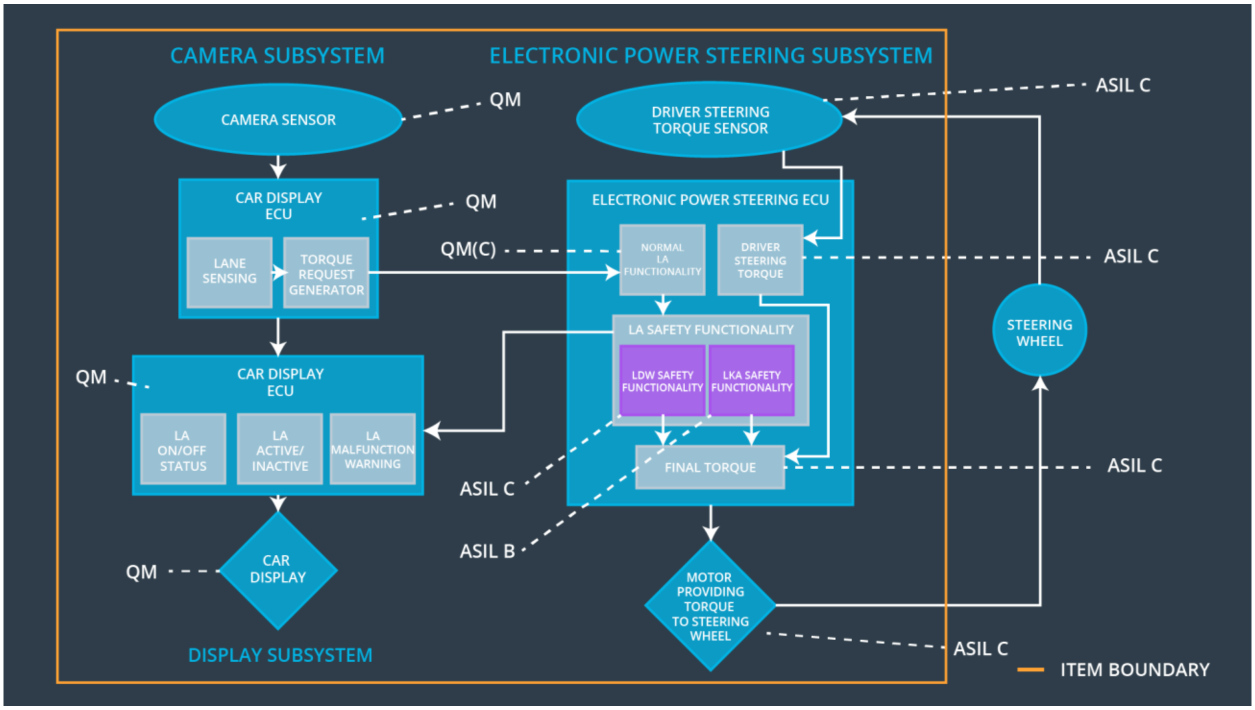
ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the it stops applying the steering torque to direct car towards the center of the lane after a certain amount of time.	B	500ms	Deactivate the function
Functional Safety Requirement 02-02	The lane assistance item shall ensure that it stops working in weather conditions where camera sensor fails.	A	10ms	Deactivate the function

Functional Safety Requirement 02-03	The lane assistance item shall ensure that it takes wind force into account while computing required torque for car steering.	C	10 ms	Alert the driver with alarm and verify driver is in control.

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	Test and validate that the Max_Duration chosen really did 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.
Functional Safety Requirement 02-02	Test and validate that Lane_Confidence_Low signal is fired when camera sensor output is not passing a confidence threshold value.	Verify that the system really does turn off if the lane keeping assistance has Lane_Confidence_Low true.
Functional Safety Requirement 02-03	Test and validate that wind direction sensor, (integrated with the power steering ECU maybe, is not part of provided system architecture diagram) can handle the situation as well as the alarm for driver works.	Verify that the system really does alarm the driver about wind situation and verifies that driver is in control by detecting steering movement.

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 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 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**		
Functional Safety Requirement 02-02	The Electronic Power Steering ECU shall ensure that the lane keeping assistance switches off when camera sensor fails.	**x**		
Functional Safety Requirement 02-03	The Electronic Power Steering ECU shall ensure that the lane keeping assistance torque also takes wind force into account	**x**		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the LDW function	Malfunction_01	Yes	Warning on Car display dashboard
WDC-02	Turn off the LKA function	Malfunction_02	Yes	Warning on Car display dashboard
WDC-03	Turn off the LDW function	Malfunction_03	Yes	Warning on Car display dashboard
WDC-04	Turn off the LDW function	Malfunction_04	Yes	Warning on Car display dashboard
WDC-05	Alarm the driver to be in control.	Malfunction_05	Yes	Warning on Car display dashboard