Functional Safety Concept Lane Assistance

Document Version: 2.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
16.02.2018	1.0	VIvanov	Draft version
19.02.3018	2.0	VIvanov	Completed document before submit

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept is looking at the item from a higher level of architecture without going into technical details.
Functional safety requirements have a few attributes that need to be specified in the functional safety concept:

- The ASIL level
- The fault tolerant time interval, which measures how quickly a system needs to react to a hazardous situation

- The safe state, which discusses what a system looks like after it has avoided an accident

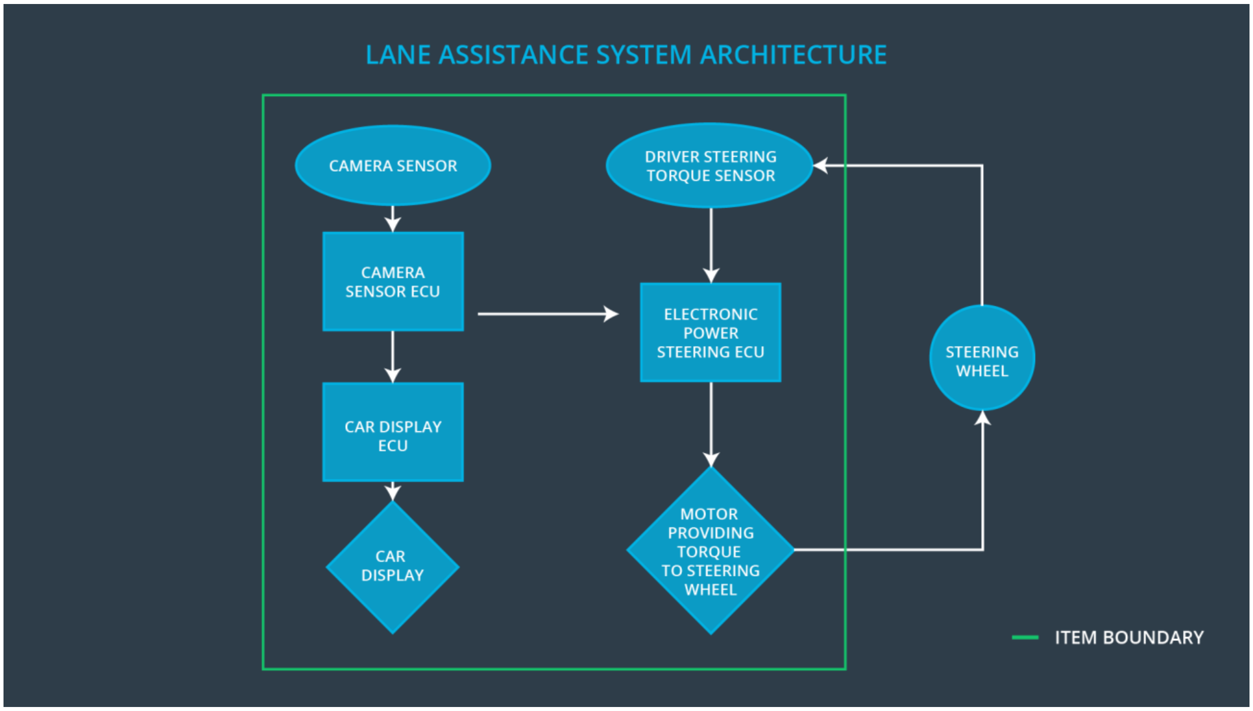
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from Lane Departure Warning function shall be limited
Safety_Goal_02	Lane Keeping Assistance function shall be time limited and the additional steering torque shall end after a given timer interval so that the driver can not misuse the system for autonomous driving
Safety_Goal_03	Lane Keeping Assistance function shall be deactivated, when camera sensor is not able to detect lane boundary. Deactivated status shall be displayed to the driver
Safety_Goal_04	Lane Departure Warning function shall control not only lane boundaries, but also traffic in neighbor lanes

Preliminary Architecture

The following figure shows the Lane Assistance item architecture


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	Image Processing and providing images to Camera Sensor ECU
Camera Sensor ECU	Object perception and recognition, detection of lane boundaries, evaluation of car position in the lane and generation of torque request to the Electronic Power Steering ECU
Car Display	Displaying of Lane Assistant item state, activity and warning messaged to the driver
Car Display ECU	Generating of warning messages triggered by Camera Sensor ECU and Electronic Power Steering ECU
Driver Steering Torque Sensor	Measuring of torque applied to the steering wheel by the driver to Electronic Power Steering ECU
Electronic Power Steering ECU	Processing of inputs from Camera Sensor ECU, Driver Steering Torque Sensor and the torque request from the Lane Keeping Assistance and Lane Warning,

	evaluating of final torque to be applied by motor
Motor	Applying the torque evaluated by the Electronic Power Steering ECU

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**	**Resulting Malfunction**
Malfunction_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	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	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	Lane Keeping Assistance function is not limited in time duration which lead 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	Lane Keeping Assistance function shall be deactivated, when camera sensor is not able to detect lane boundary
Malfunction_05	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	LATE	Lane Departure Warning function shall control not only lane boundaries, but also traffic in neighbor lanes

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 amplitude is below Max_Torque_Amplitude	C	50ms	Lane departure oscillating torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50ms	Lane departure oscillating torque frequency is below Max_Torque_Frequency
Functional Safety Requirement 01-03	Lane Departure Warning function shall ensure that the distance to obstacle left or right is more than Min_Obstacle_Distance	C	10ms	Distance to obstacles on sides are more than Min_Obstacle_Distance

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 chosen Max_Torque_Amplitude value is high enough to be detected by driver and low enough to continue control of steering	Verify the system does turn off the Lane Departure Warning function when exceeded Max_Torque_Amplitude
Functional Safety Requirement 01-02	Validate, that chosen Max_Torque_Frequency value is high enough to be detected by driver and low enough to continue control of steering	Verify the system does turn off the Lane Departure Warning function when exceeded Max_Torque_Frequency
Functional Safety Requirement 01-03	Validate, that chosen Min_Obstacle_Distance is low enough to still be in lane center and high enough to still have safe control of vehicle (as reference, values can be obtained from Traffic Laws)	Verify the system does turn on the Lane Departure Warning function when reached Min_Obstacle_Distance

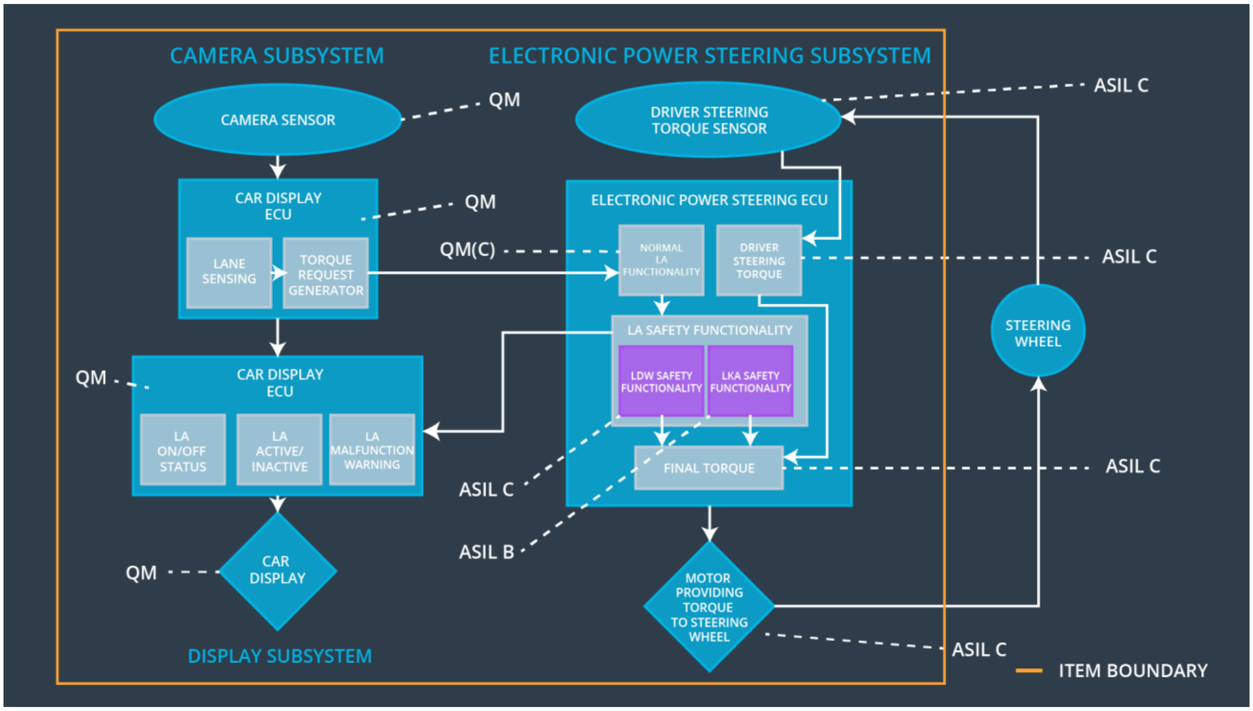
Lane Keeping Assistance (LKA) Requirements:

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	500ms	Lane Keeping Assistance is deactivated
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the camera sensor is not able to detect lane boundaries not long, than Max_Not_Observable_Time	A	10ms	Lane Keeping Assistance is deactivated

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 chosen Max_Duration is high enough to be detected by driver and low enough to not feel the function is for autonomous drive	Verify the system does turn off the Lane Keeping Assistance function when reached Max_Duration
Functional Safety Requirement 02-02	Validate, that chosen Max_Not_Observable_Time is big enough for real road situations on intersections and low enough to have time of keep control of vehicle in case the function is deactivated	Verify the system does turn off the Lane Keeping Assistance function and warn the driver when reached Max_Not_Observable_Time

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 lane keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude	**X**		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	**X**		
Functional Safety Requirement 01-03	Lane Departure Warning function shall ensure that the distance to obstacle left or right is more than Min_Obstacle_Distance	**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	The electronic power steering ECU shall ensure that the camera sensor is not able to detect lane boundaries not long, than Max_Not_Observable_Time	**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	Yes	Lane Assistance malfunction Warning

WDC-02	Turn off Lane Departure Warning functionality	Malfunction_02	Yes	Lane Assistance malfunction Warning
WDC-03	Turn off Lane Keeping Assistance functionality	Malfunction_03	Yes	Lane Assistance malfunction Warning
WDC-04	Turn off Lane Keeping Assistance functionality	Malfunction_04	Yes	Lane Assistance malfunction Warning
WDC-05	Turn off Lane Departure Warning functionality	Malfunction_05	Yes	Lane Assistance malfunction Warning