Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: Version 1.1, Released on 2018-11-21

Document history

Date	Version	Editor	Description
11/18/18	1.0	Emile Papillon	First draft
11/21/18	1.1	Emile Papillon	Review and release

Table of Contents

Purpose of the Functional Safety Concept

The functional safety concept refines the safety goal and derives functional safety requirements. These requirements are then allocated to systems components in the systems diagram showing where each safety requirements will be implemented. The resulting architecture may differ from the preliminary architecture. Functional safety requirements are given the following attributees : ASIL level, Fault Tolerant Time Interval (FTTI) and the safe state.

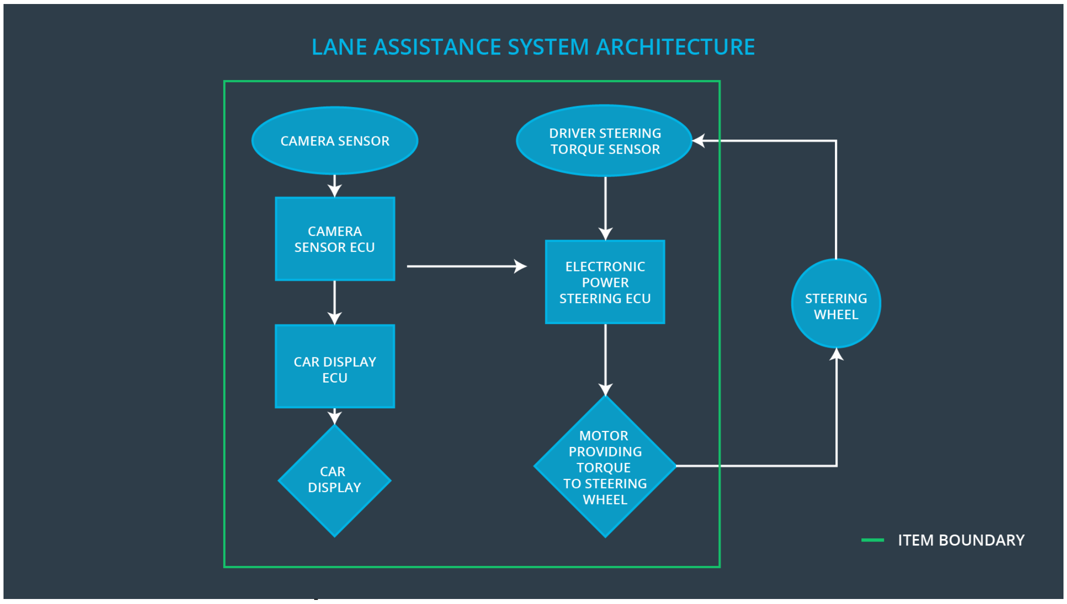
Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

The following safety goals are the results of the Hazard and Risk Analysis (HARA) .

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.
Safety_Goal_03	The lane assistance system shall turn off when the driver turns on the hazards.
Safety_Goal_04	The lane warning feature shall be deactivated if the camera sensor has a fault.

Preliminary 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

Element	Description
Camera Sensor	Responsible for detecting the lines
Camera Sensor ECU	Responsible of processing the data captured by the camera sensor and determining when the vehicle leaves the lane by mistake
Car Display	Interface with the human driver displaying system status and fault/malfunction warnings
Car Display ECU	Interface between the lane assistance system and the car display
Driver Steering Torque Sensor	Senses the torque input by the driver to provide just the right amount of extra torque for lane keeping assistance
Electronic Power Steering ECU	Interface between the driver torque sensor and the motor to calculate and apply the right amount of torque
Motor	Applies torque to the steering wheel/column.

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 malfunctions and applies an oscillating torque with very high intensity (above expected level from human user).
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.
Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego	NO	The Lane Keeping Assistance function is not limited in time duration which lead to misuse
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	Lane keeping keeps applying lane centering torque while the driver is trying to pull off to shoulder
Malfunction_05	Lane Departure Warning (LDW) function shall apply an oscillating steering	WRONG	Malfunction in camera subsystem causes lane departure warning to trigger off at random

	torque to provide the driver a haptic feedback.		moments

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 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.	C	50 ms	Vibration frequency is below Max_Torque_Frequency.
Functional Safety Requirement 01-03	The Lane Keeping Feature shall turn off if a fault is detected in the camera subsystem	B	50 ms	Lane Keeping Turns off when there is a fault in the camera subsystem

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 chosen amplitude threshold Max_Torque_Amplitude is low enough to make the system safe.	Make sure that under no circumstances the system applied torque exceed Max_Torque_Amplitude
Functional Safety	The chosen frequency Max_Torque_Frequency is low	Make sure that under no circumstances the system rate of

Requirement 01-02	enough to make the system safe	vibration exceeds Max_Torque_Frequency
Functional Safety Requirement 01-02	Disabling the system every time there is a fault in the camera system ensures the safety of the user.	Introduce many different faults in the camera subsystem and make sure the LDW feature is disabled

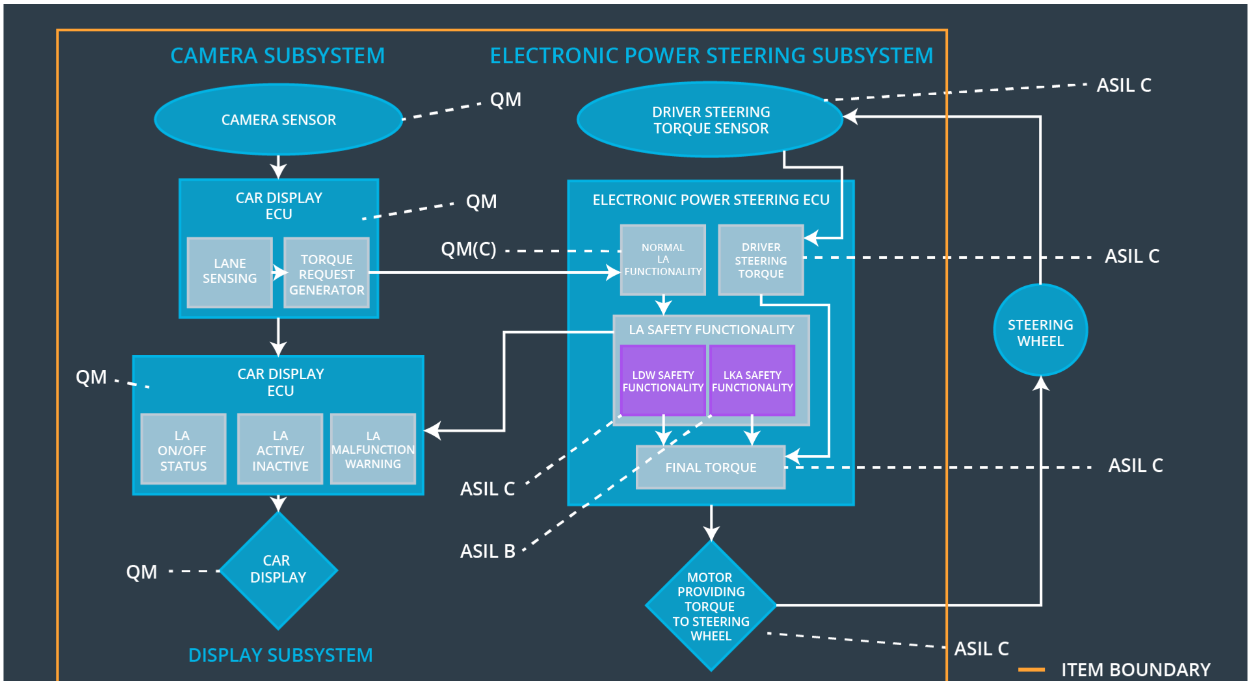
Lane Keeping Assistance (LKA) Requirements:

ID	**Functional Safety Requirement**	**ASIL**	**Fault Tolerant Time Interval**	**Safe State**
Functional Safety Requirement 02-01	The Lane Keeping Assistance shall be limited in time to a duration of Lane_Keeping_Timeout after which the feature turns off	B	50 ms	Lane Keeping turns off after Lane_Keeping_Timeout

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	The duration Lane_Keeping_Timeout effectively makes the driver less likely to misuse the system	Make sure that in every possible use case the lane keeping does not exceed Lane_Keeping_Timeout seconds.

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 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	The Lane Keeping Feature	X		

Safety Requirement 01-03	shall turn off if a fault is detected in the camera subsystem			
Functional Safety Requirement 02-01	The Lane Keeping Assistance shall be limited in time to a duration of Lane_Keeping_Timeout after which the feature turns off	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 completely	Malfunction_01, Malfunction_02, Malfunction_05	Yes	LDW malfunction Warning light on Car Display
WDC-02	Turn off Lane Keeping Assistance functionality completely	Malfunction_03, Malfunction_04, Malfunction_05	Yes	LKA malfunction Warning light on Car Display