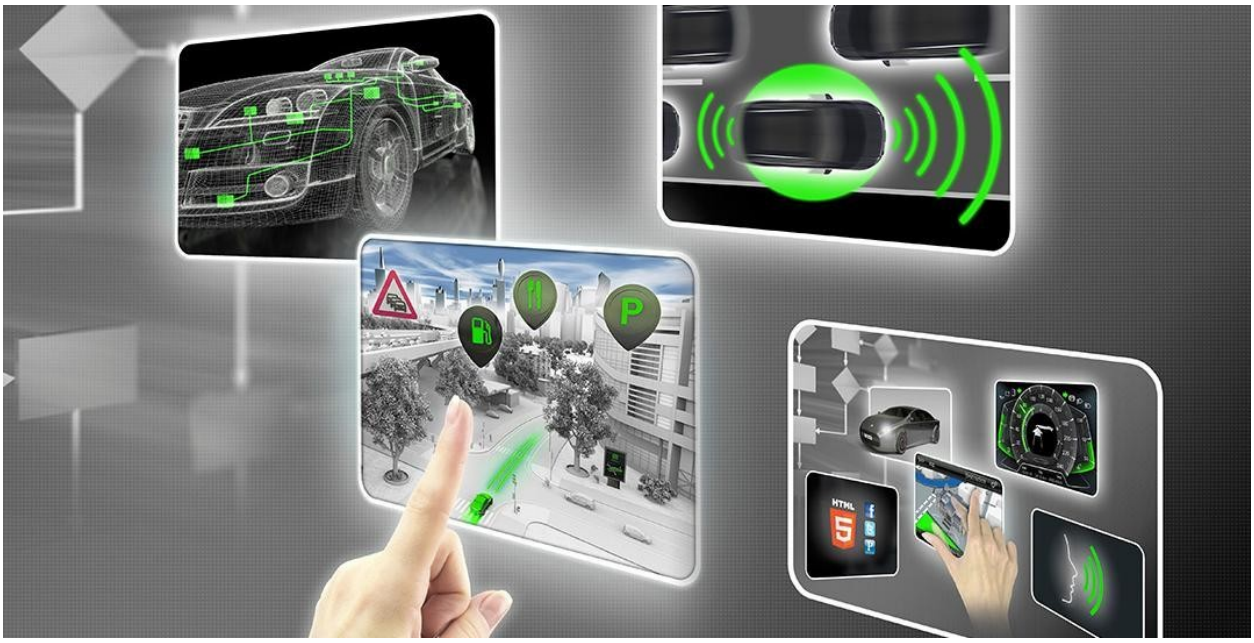
Functional Safety Concept Lane Assistance

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
2019-01-03	1.0	Simon Beyer	Initial draft

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]

Purpose of the Functional Safety Concept

[Instructions: Answer what is the purpose of a functional safety concept?]
The functional safety concept looks at the general functionality of the Lane Assistance item. This document refines the safety goals into functional safety requirements. These functional safety requirements have the following attributes:

- 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

The functiona safety concept also includes verification and validation.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

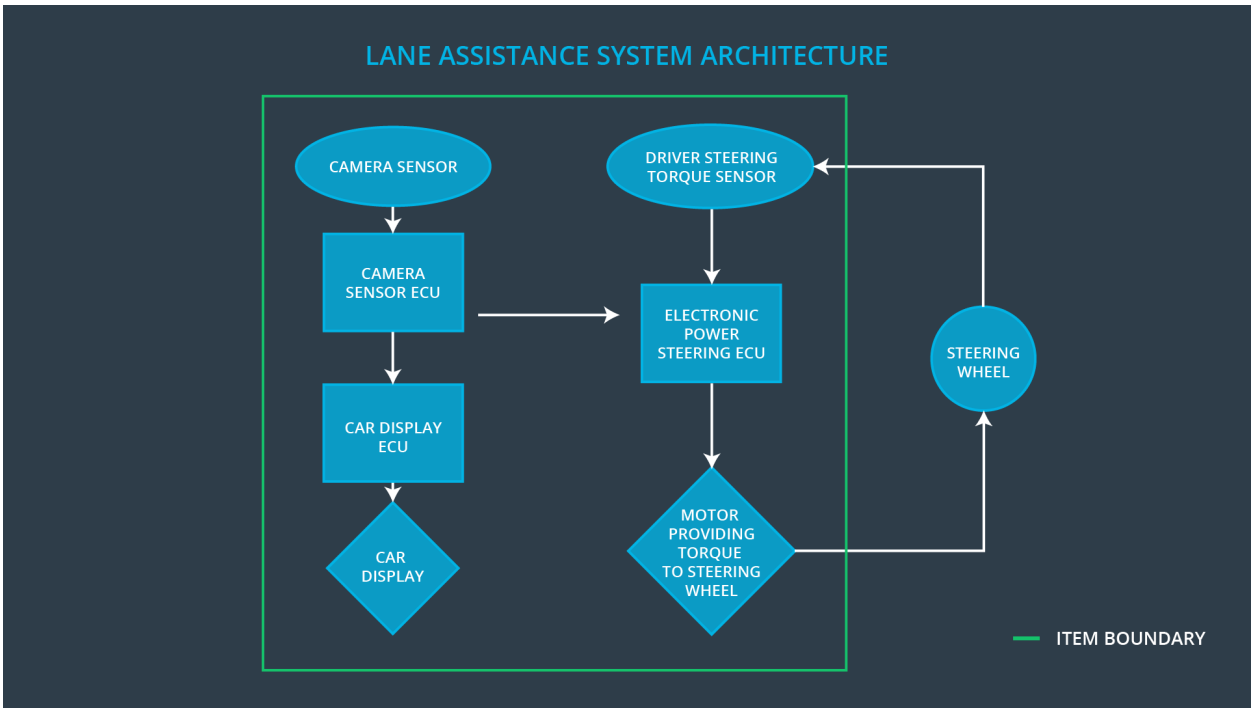
[Instructions:
REQUIRED:
Provide the lane departure warning and lane keeping assistance safety goals as discussed in the lessons and derived in the hazard analysis and risk assessment.

OPTIONAL:
If you expanded the hazard analysis and risk assessment to include other safety goals, include them here.
]

ID	Safety Goal
Safety_Goal_01	The oscillating torque to the steering wheel 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
Safety_Goal_03	The electronic power steering ECU shall check that the acutal provided steering torque is only a few ms behind the demanded torque. If the actual torque is provided too late the steering support torque shall end.
Safety_Goal_04	The electronic power steering ECU shall check whether the indicated driver steering torque from the sensor is plausible (e.g. with a model based approach). If the indicated driver steering torque is not plausible the support torque shall end.

Preliminary Architecture

[Instructions: Provide a preliminary architecture for the lane assistance item. Hint: See Lesson 3: Item Definition]



Description of architecture elements

[Instructions: Provide a description for each of the item elements; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	The camera sensor reads in images from the road.
Camera Sensor ECU	The Camera Sensor ECU identifies when the vehicle has accidentially departed its lane, and sends the appropriate messages to the Car Display ECU and the Electronic Power Steering ECU.
Car Display	The Car Display shows a warning light to the driver, when the vehicle leaves the lane.
Car Display ECU	The Car Display ECU turns on the warning light on the Car Display when it receives information from the Camer Sensor ECU that the vehicle is leaving the lane.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor provides the torque that the driver puts on the steering wheel to the Electronic Power Steering ECU.
Electronic Power Steering ECU	The Electronic Power Steering ECU reads the info from the Driver Steering Torque Sensor and commands a support torque from the Motor, based on the lane infor from the Camera Sensor ECU.
Motor	The Motor applies the demanded torque that is demanded by the Electronic Power Steering ECU onto 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	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

[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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50 ms	Turn off the funcionality – Set torque request to 0
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency.	C	50 ms	Turn off the funcionality – Set torque request to 0

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	Make a study to test how drivers react to different torque amplitudes to prove that we chose an appropriate value.	Do a software test by inserting a fault into the system. When the demanded torque amplitude crosses the limit, the lane assistance output must be set to zeros within 50 ms.
Functional Safety Requirement 01-02	Make a study to test how drivers react to different torque frequencies to prove that we chose an appropriate value.	Do a software test by inserting a fault into the system. When the demanded torque frequency crosses the limit, the lane assistance output must be set to zeros within 50 ms.

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

Lane Keeping Assistance (LKA) Requirements:

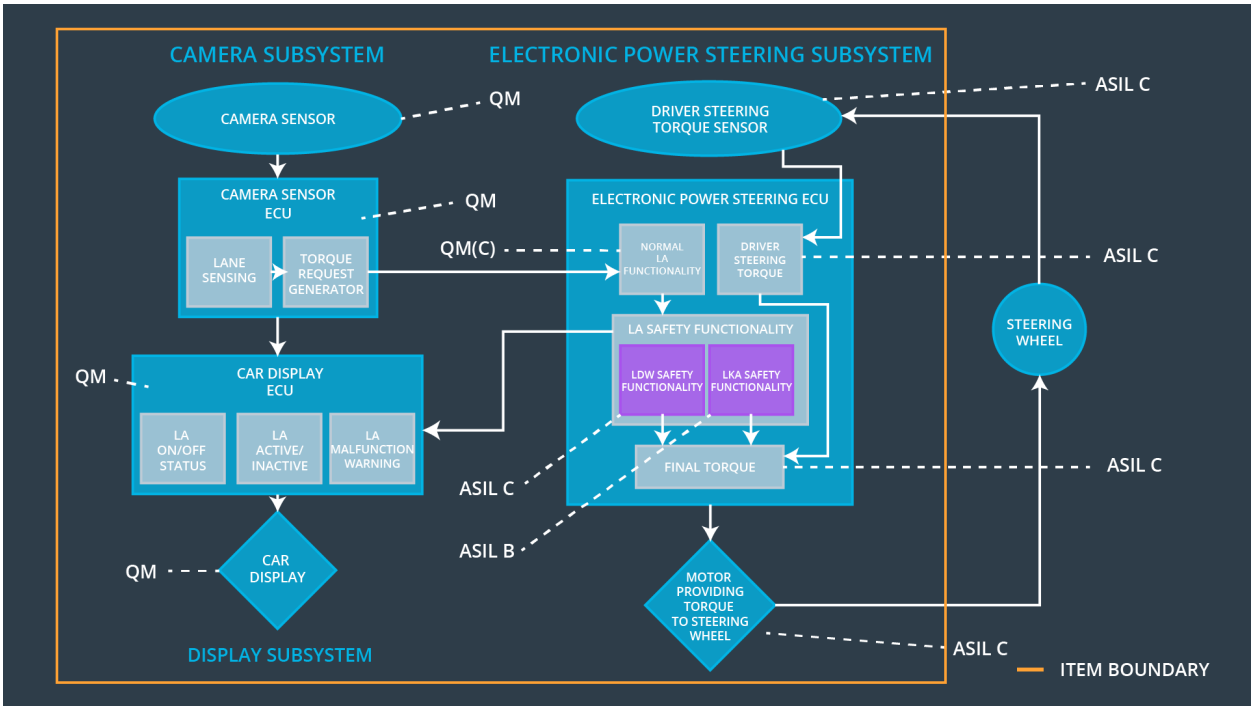
ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only ‘Max_Duration’.	B	500 ms	Turn off the funcionality – Set torque request to 0

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	Make a study to test that the time ‘Max_Duration’ chosen really dissuades drivers from taking their hands off the wheel.	Make car or software tests that the system really does turn off if the lane keeping assistance ever exceeded ‘Max_Duration’.

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the functional safety lesson including all of the ASIL labels.]



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 keeping item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	**x**		
Functional Safety Requirement 01-02	The Electronic Power Steeriing ECU shall ensure that the oscillating torque frequency requested by the LDW function 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

[Instructions: Fill in the warning and degradation concept.]

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off the funcionality – Set torque request to 0	The lane departure warning function applies an oscillating torque with very high torque amplitude or torque frequency (above limit).	Yes	A message on the car display shows the driver, that the lane departure warning function is not available.
WDC-02	Turn off the funcionality – Set torque request to 0	The lane keeping assistance function is not limited in time duration which leads to misuse as an autonomous driving function.	Yes	A message on the car display shows the driver, that the lane keeping assistance function is not available.