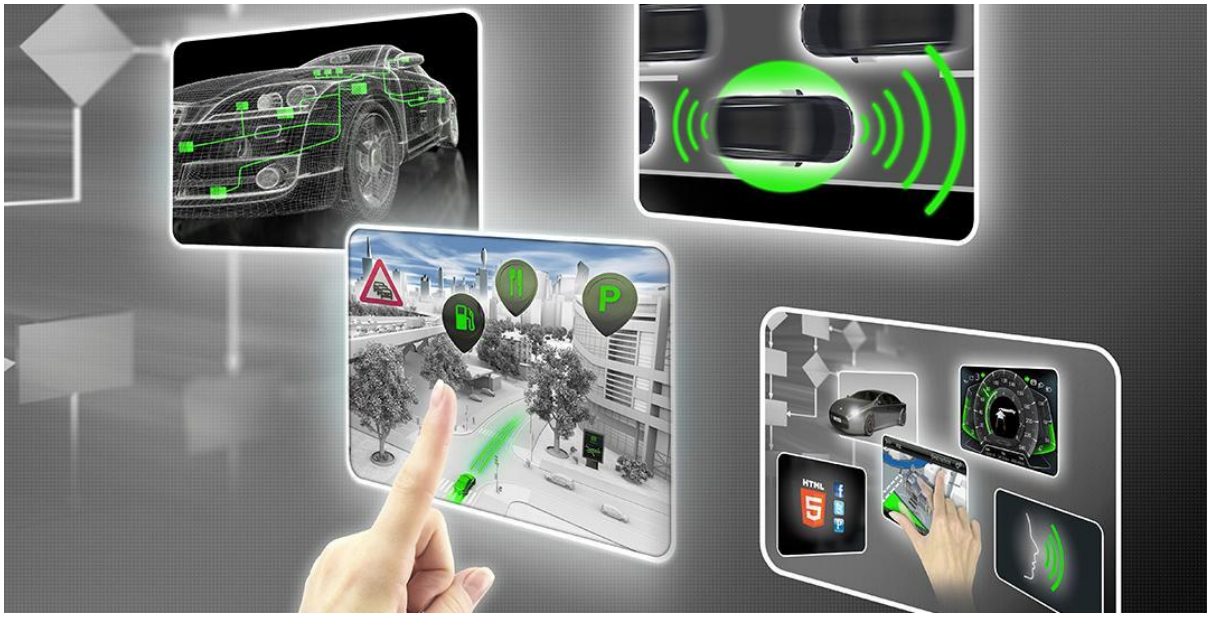
Elektrobit

UDACITY

Functional Safety Concept
Lane Assistance

Document Version: 0.1

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
2017-09-09	0.1	Olli Vertanen	Initial version.

Table of Contents

Purpose of the Functional Safety Concept

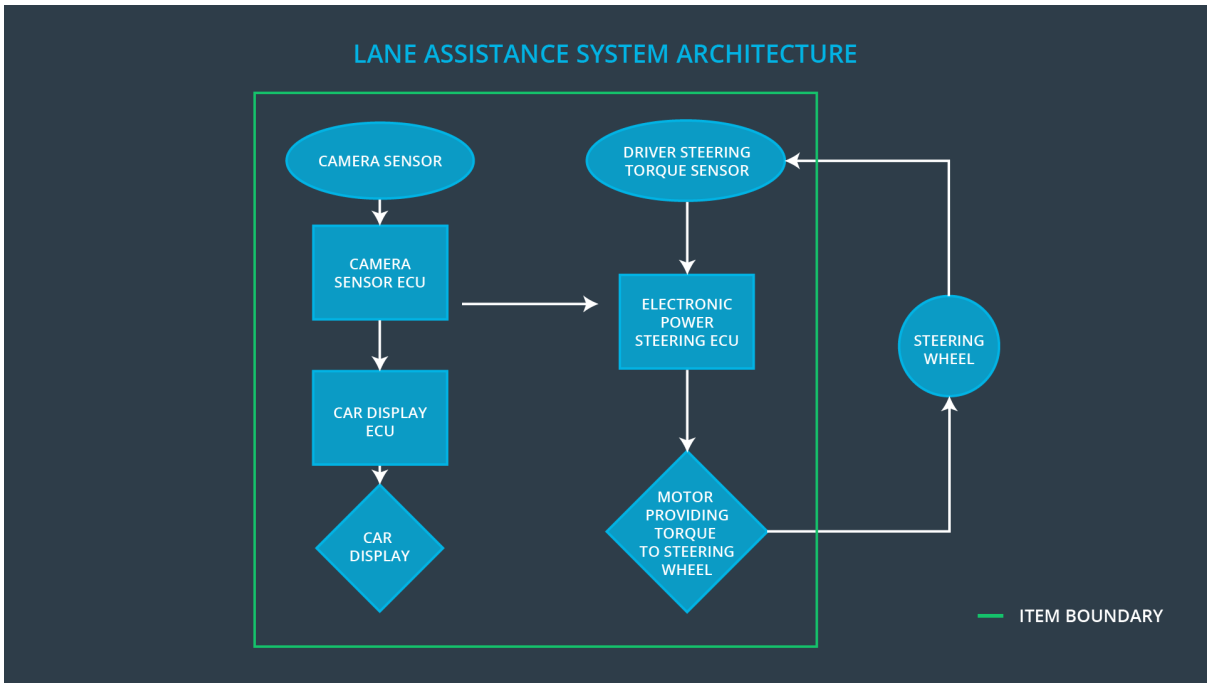
The purpose of functional safety concept is to derive the functional safety requirements from the safety goals (produced in hazard analysis and risk assessment), and to allocate them to the preliminary architectural elements of the item (or to external measures).

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 LDW function shall be limited.
Safety_Goal_02	The LKA function shall be time limited and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving.
Safety_Goal_03	The corrective steering torque of the LKA function must always be towards the centre of the ego lane.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Provides images of the road ahead of the vehicle.
Camera Sensor ECU	Detects lanes from images. Calculates vehicle's position within the ego lane.
Car Display	Display warning/alarm indicators.
Car Display ECU	Controls display unit.
Driver Steering Torque Sensor	Senses the torque that driver is applying to steering wheel.
Electronic Power Steering ECU	Calculates needed steering torque.
Motor	Provides torque to 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) 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.
Malfunction_04	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	WRONG	The lane keeping assistance function applies steering torque to the opposite direction than needed in order to stay in ego lane.

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	50 ms	LDW turned off
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	LDW turned off

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	Test the LDW function with different torque amplitudes and with different drivers. Measure the amplitudes and analyse drivers' reactions. Deduce from the reactions what is a safe Max_Torque_Amplitude.	Inject a fault that raises oscillating torque amplitude above Max_Torque_Amplitude. Item should go to safe state within FTTI.
Functional Safety Requirement 01-02	Test the LDW function with different torque frequencies and with different drivers. Measure the frequencies and analyse drivers' reaction. Deduce from the reactions what is a safe Max_Torque_Frequency.	Inject fault that raises oscillating torque frequency above Max_Torque_Frequency. Item should go to safe state within FTTI.

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 lane keeping assistance torque is applied for only Max_Duration.	B	500 ms	LKA turned off
Functional Safety Requirement 02-02	The lane keeping item shall ensure that the lane keeping assistance torque has same direction than Lane_Centre_Distance. The ego lane centre is on the left (driving direction), if the distance is negative.	B	50 ms	LKA turned off

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria

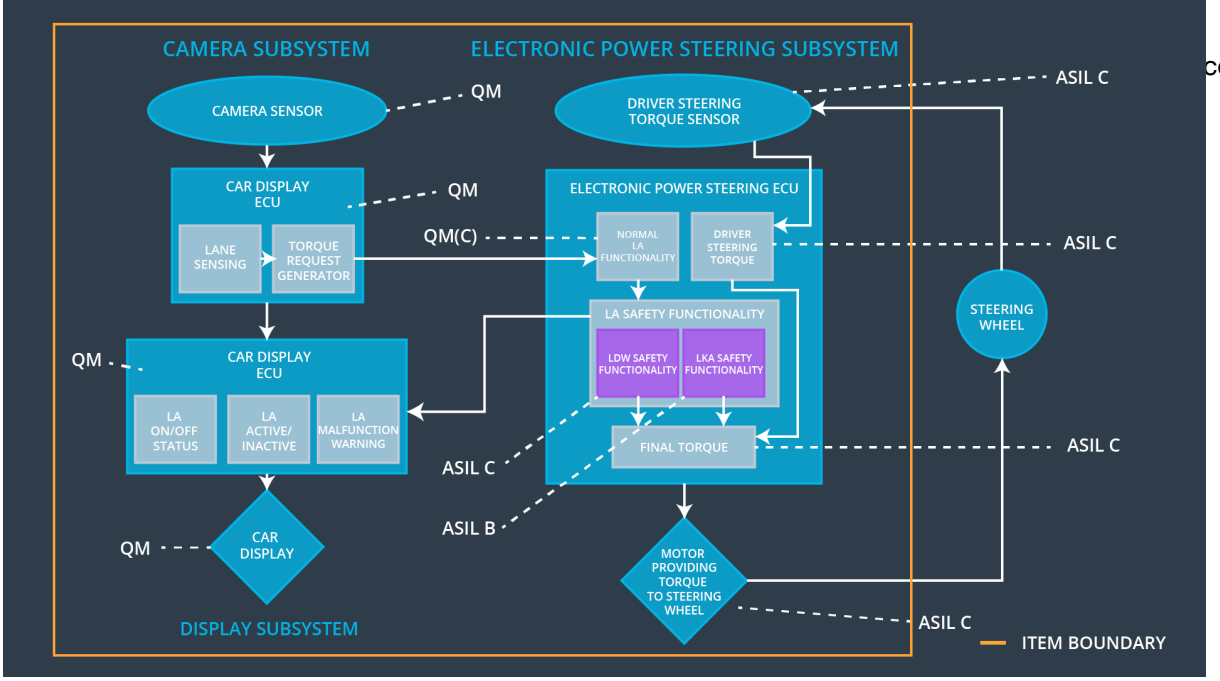
ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	Test the LKA function with different torque duration and with different drivers. Measure the frequencies and drivers' reaction. Deduce from the reactions what is a safe Max_Torque_Duration.	Verify by testing in real driving conditions that after activation LKA is turned off within the defined limit.
Functional Safety Requirement 02-02	Validate in real driving conditions that the direction of the assisting torque should be towards the centre of the ego lane.	Verify by testing in real driving conditions, that the direction of the assisting torque is correct.

Refinement of the System Architecture

All safety related functional requirements are allocated to electronic power steering subsystem (see next chapter). Thus the whole sub-system inherits the highest ASIL of the requirements, ASIL C. Because there are not special functional safety requirement for the other two sub-systems, these can be marked as QM.

Further, lane assistant functionality of the electronic power steering ECU should be labelled as ASIL C, because this is the highest ASIL inherited from the allocated functional safety requirements. In the architecture, the functionality is decomposed, using ASIL decomposition rules, to normal lane assistant functionality and safety critical lane assistant functionality. Further, the safety critical lane assistant functionality is divided to two sub-blocks: lane departure warning functionality and lane keeping assistance functionality. According to criteria for co-existence, we can assign ASIL B to the lane keeping assistance functionality, if the lane keeping assistance does not interfere with the lane departure warning functionality.

This reasoning leads us to the following refined architecture with ASIL labels.



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 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 torque has same direction than Lane_Centre_Distance. The ego lane centre is on the left (driving direction), if the distance is negative.	**X**		

Warning and Degradation Concept

The warning and degradation concept discusses, how the driver will be warned of a malfunction and what the system will do to take the system to a safe state and also recover from a safe state.

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW	Malfunction_01 Malfunction_02	Yes	Dashboard light
WDC-02	Turn off LKA	Malfunction_03 Malfunction_04	Yes	Dashboard light