Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
12.01.2019	1.0	Michael Ikemann	Initial definition of functional safety

Table of Contents

Document history

Table of Contents

Purpose of the Functional Safety Concept

Inputs to the Functional Safety Analysis
- Safety goals from the Hazard Analysis and Risk Assessment
- Preliminary Architecture
  - Description of architecture elements

Functional Safety Concept
- Functional Safety Analysis
- Functional Safety Requirements
- Refinement of the System Architecture
- Allocation of Functional Safety Requirements to Architecture Elements
- Warning and Degradation Concept

Purpose of the Functional Safety Concept

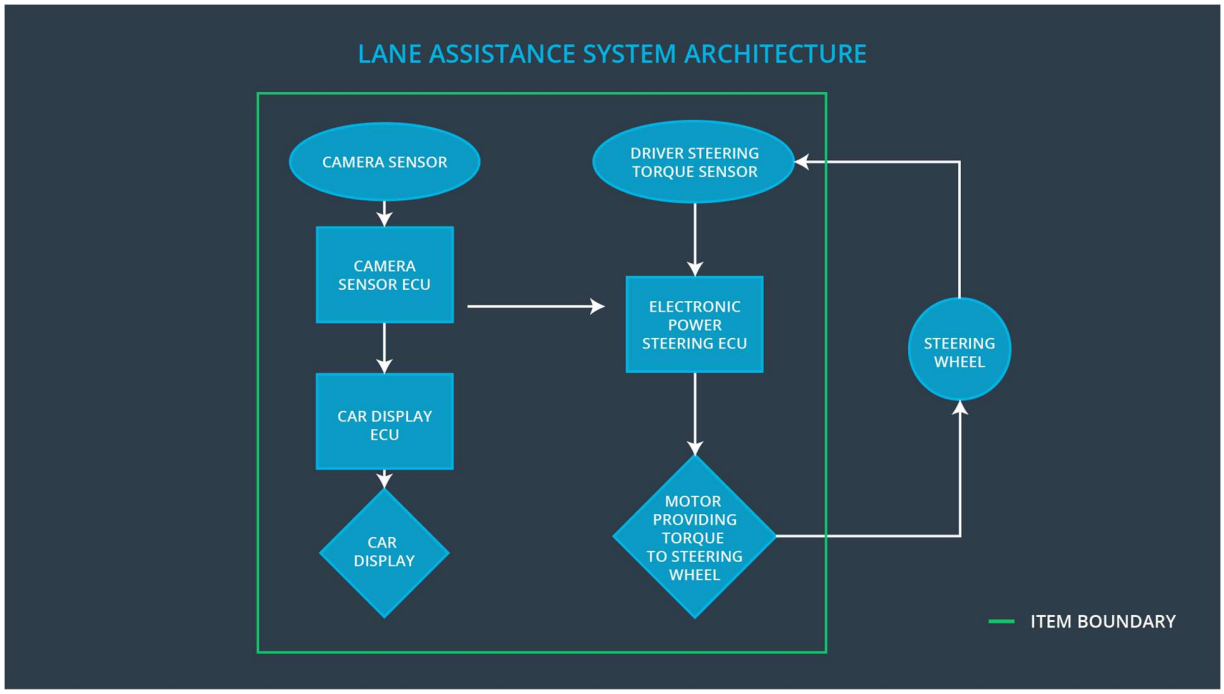
The purpose of the functional safety concept is to define the single functionalities from a high level perspective, how the the safety can be ensured as much as possible for each of it's features and the functionality's ASIL level.

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The vehicle should detect bad weather conditions and inform the other that the system's functionality might be limited and/or should automatically be disabled after informing the user in cases where for example the sensors are covered by snow and not fully functional.
Safety_Goal_02	The vibration of the steering while should be limited in all involved components to prevent accidents caused by a scared driver.
Safety_Goal_03	If the user removes the hands from the steering wheel the driver should be informed audiovisual that the lane guidance will be deactivated because the system shall not be used in an autonomous manner.
Safety_Goal_04	It shall be verified that the lane guidance system will be disabled when the vehicle is not driving.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Captures the image. Is mounted at the top of the wind screen.
Camera Sensor ECU	Analyses the image – detects the lane and the detection certainty and decides if the user shall be warned about lane departure or follow the center of the lane if lane guidance is activated.
Car Display	Visualizes if lane guidance and departure features are activated and also informs the user when a lane departure occurs.
Car Display ECU	Is responsible for the visualization of the car's dashboard. Needs to be extended for the visualization of LGA related features.
Driver Steering Torque Sensor	Detects with which amount of force the driver tries to steer. In case of the LGA a non-existing steering of the driver in a curve should lead to a warning so the driver will not use the LGA in an autonomous way. Also a

	counter-steering of the driver should be detected and disable the lane guide so the driver will regain control of the vehicle if required.
Electronic Power Steering ECU	The EPS ECU decides by the information provided by the DSTS and CS ECU which amount of torque to apply to the steering wheel.
Motor	Applies the amount of torque provided by the EPS ECU to the steering wheel so that the vehicle will (for example) follow the lane detected.

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	The lane departure warning applies more oscillating torque than intended.	A too strong vibration of the steering wheel would distract the driver.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	The computation of the camera ECU arrives too late at the EPS ECU.	The driver will be notified too late to still be able to react due to a delayed notification.

Malfunction_03	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	The LKA steers wrongly within a road work site due to crossing lane markers which irritated the CS ESU.	The vehicle drives into a wrong direction and potentially causes an accident.

Functional Safety Requirements

Lane Departure Warning (LDW) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	Bad weather conditions and incorrectly working sensors are detected and the user will be informed.	B	0.1	The system will be disabled and the user will be informed about it's state.
Functional Safety Requirement 01-02	The detection data is provided in intervals of 10 Hz. In case of lost messages the system will automatically be disabled.	B	0.1s	The user will be informed that the system works incorrectly and the LDW will be disabled and it's status shown in the dash board.

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 vehicle will be tested under several weather conditions and the sensors intentionally blocked.	When ever a sensor can not guarantee it's correct functionality anymore due to crosschecks with other sensors the system automatically gets disabled.
Functional Safety Requirement 01-02	The receiving units verify that status updates from the CS ECU arrive in the correct order in time intervals of 10 Hz.	The communication will intentionally be disturbed and the CS disabled. The system should be automatically disabled when status updates due not

	The CRC checksum computed at the receiver matches the provided checksum.	arrive in time.

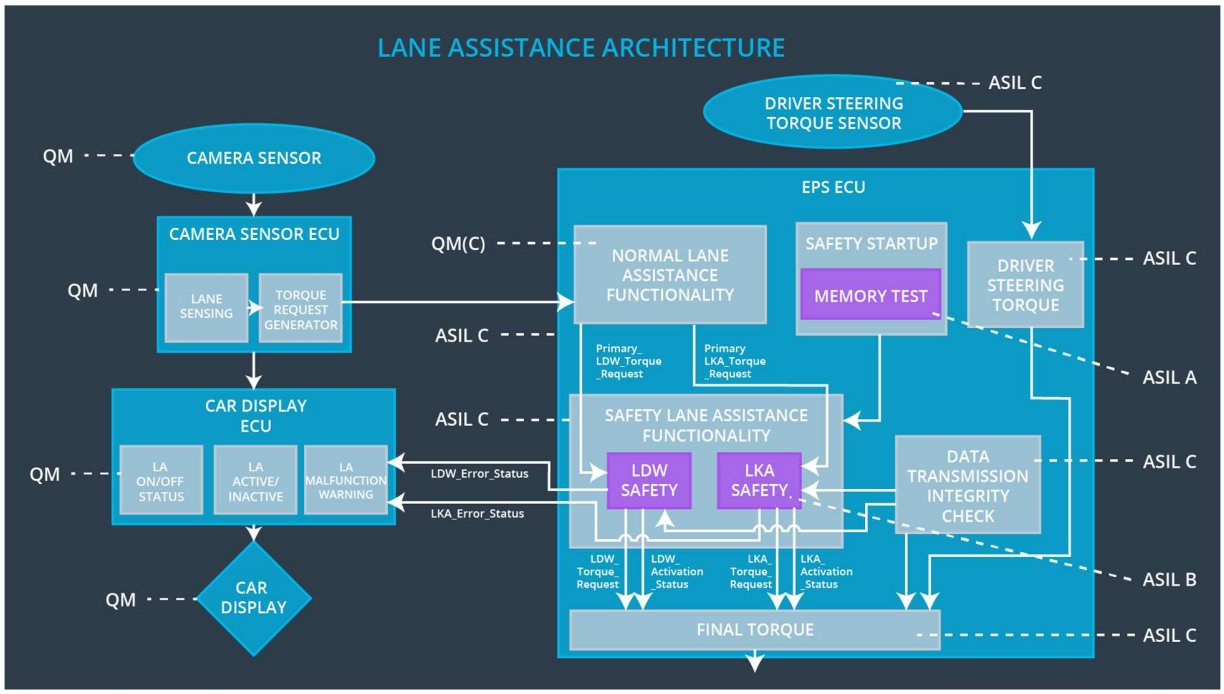
Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	If the current situation can be detected reliably anymore the system should slow down the car and instantly inform the driver.	B	0.1	The LKA is disabled and the user informed via the dashboard and a warning signal in the dashboard

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	In situations where it can not clearly detect the correct lanes anymore such as in road work sites it should temporarily be disabled.	The car is tested in several different situations and correctly informs the user when it can not reliably support the lane guidance.

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	Bad weather conditions and incorrectly working sensors are detected and the user will be informed.		**Detects sensor failures in disables the LDW.**	**Informs the driver that the LDW has been disabled.**
Functional Safety Requirement 01-02	The detection data is provided in intervals of 10 Hz. In case of lost messages the system will automatically be disabled.	**Detects incorrect transmissi ons**		**Informs the driver that the LDW has been disabled.**
Functional Safety Requirement 02-01	In situations where it can not clearly detect the correct lanes anymore such as in road work		**Automati cally detects uncertain**	**Informs the driver that the LKA does not support at the**

	sites it should temporarily be disabled		**situations and stops taking control if it could lead to an accident.**	**moment.**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Disabled until next motor start.	CRC checksum errors in communication and or no data provided at 10 Hz rate as required.	LDW disabled.	Error light in dashboard.
WDC-02	Disabled temporarily till situation is safe again.	Too many, none or contradictionary lanes detected.	LKA temporarily disabled.	Inactivity visualized in dashboard.