Functional Safety Concept Lane Assistance

Document Version: 1.1

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
12-26-18	1.0	Nick Fiege	
01-01-19	1.1	Nick Fiege	Changed Safe State for Functional Safety Requirement 01-01 and 01-02 after submission.

Table of Contents

Document history....................2
Purpose of the Functional Safety Concept....................3
Inputs to the Functional Safety Concept....................3
Safety goals from the Hazard Analysis and Risk Assessment....................3
Preliminary Architecture....................4
Description of architecture elements....................4
Functional Safety Concept....................5
Functional Safety Analysis....................5
Functional Safety Requirements....................6
Refinement of the System Architecture....................7
Allocation of Functional Safety Requirements to Architecture Elements....................8
Warning and Degradation Concept....................8

Purpose of the Functional Safety Concept

The functional safety concept describes the high level functionality of an item:

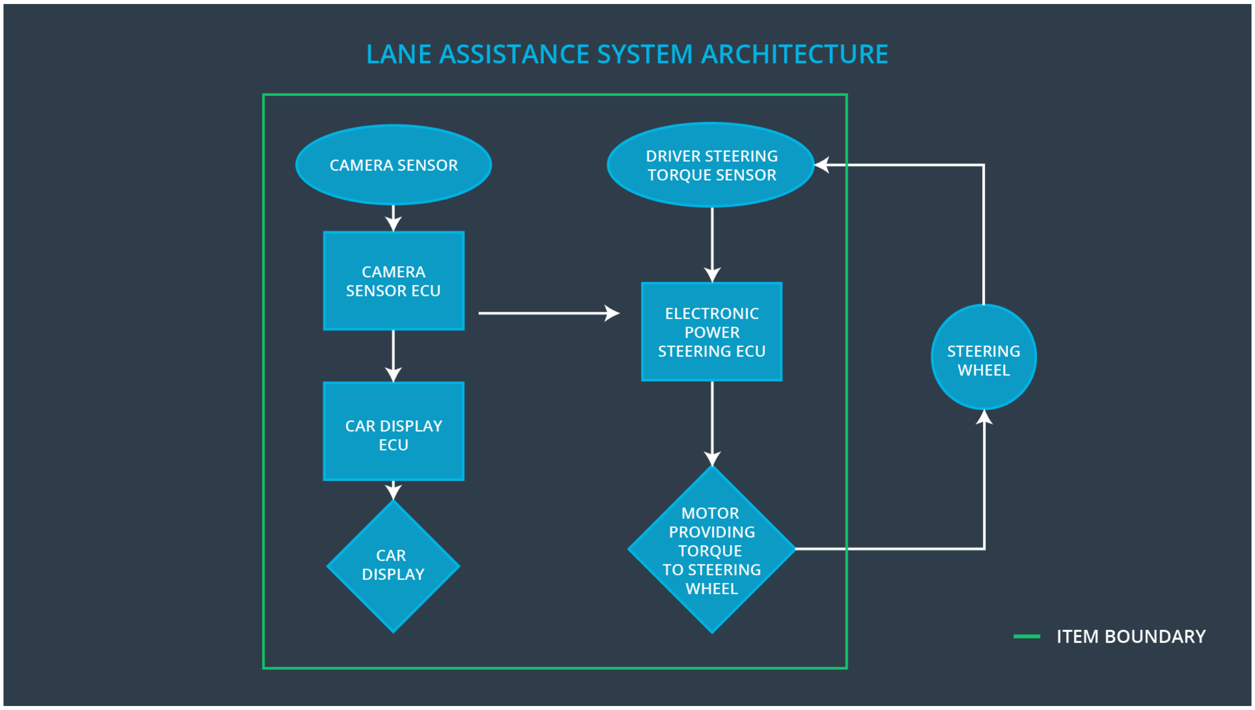
- First it needs to be defined which subsystems contain high levels of risk and what needs to be done to prevent accidents.
- Determine which subsystems and elements can be used to meet safety goals.
- Further refine these goals into functional safety requirements.
- Allocate each functional safety requirement to its appropriate place in the item architecture.
- The subsystems which have new requirements allocated to them might need to be refined, i.e. subdivided and defined in detail.
- Subsystems inherit the ASIL of the requirements and they then might be decomposed to make sure that only the safety critical elements have to be fully analysed according to its higher ASIL level.
- Instructionas are provided on the verification and validation of the requirements.

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 lane departure warning function shall be limited
Safety_Goal_02	The lane keeping assistance 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 Lane Keeping Assistance function shall be deactivated when the camera sensor information is insufficient.
Safety_Goal_04	The torque applied by the driver shall always be measured correctly within a defined accuracy.

Preliminary Architecture


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
DRIVER STEERING TORQUE SENSOR
CAMERA SENSOR ECU
ELECTRONIC POWER STEERING ECU
STEERING WHEEL
CAR DISPLAY ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
CAR DISPLAY
ITEM BOUNDARY

Description of architecture elements

Element	**Description**
Camera Sensor	Provides images which can be processed for lane assistance.
Camera Sensor ECU	Processes given images to determine vehicle odometry and lane boundarys. Sends vital control information to Electronic Power Steering ECU and user information to Car Display ECU.
Car Display	Displays warnings and general information for the driver.
Car Display ECU	Processes and interprets Camera Sensor ECU data and controls Car Display.
Driver Steering Torque Sensor	Detects exterted torque to the steering wheel.
Electronic Power Steering ECU	Takes torque requests from the camera ECU and calculates the difference between the required torque and the torque already exerted by the driver.
Motor	Applies the torque requested from the Electronic Power Steering ECU to 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

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 oscilating torque applied by the lane departure warning system has a torque amplitude above the defined limit.
Malfunction_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	MORE	The oscilating torque applied by the lane departure warning system has a torque frequency above the defined limit.
Malfunction_03	The Lane Departure Warning function shall be deactivated when the camera sensor stop working.	WRONG	The system acts unpredictable when the camera sensor is not working correctly.
Malfunction_04	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

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	Oscillating torque amplitude is set to zero.
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	Oscillating torque frequency is set to zero.

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 and calibrate the setting of max_torque_amplitude by gathering driver experiences.	Verify that the target torque for the motor never exceeds the maximum given by max_torque_amplitude.
Functional Safety Requirement 01-02	Validate and calibrate the setting of max_torque_frequency by gathering driver experiences.	Verify that the target torque for the motor never exceeds the maximum given by max_torque_frequency.

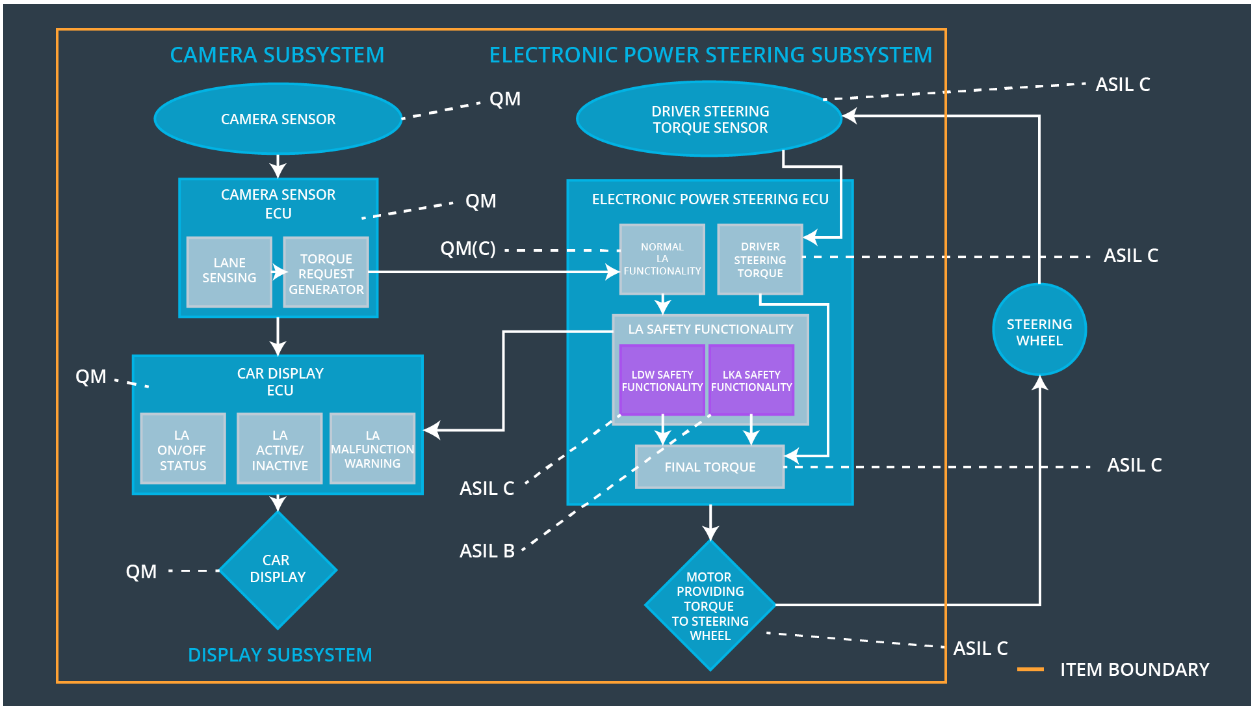
Lane Keeping Assistance (LKA) Requirements:

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 the applied torque used for maneuvering back to the center of the lane is applied for a maximum time defined by max_torque_duration.	B	500 ms	Torque is not applied anymore (set to zero).

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 the setting of max_torque_duration by gathering driver experiences so that the system is not misused as an autonomous system.	Verify that the systems turns off after max_torque_duration time is exceeded.

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 mas_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 02-01	The Electronic Power Steering ECU shall ensure that the the applied torque used for maneuvering back to the center of the lane is applied for a maximum time defined by max_torque_duration.	x		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane assistance system is turned off.	Malfunction_01 Malfunction_02 Malfunction_03 Malfunction_04	Yes	Dashboard warning light, Display warning