Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
11/20/17	0.1	My Safetyplan	Initial Draft

Table of Contents

Purpose of the Technical Safety Concept

A technical safety concept is similar to a functional safety concept in the sense that it defines requirements and allocates them to subsystems. While a functional safety concept provides a bird’s eye view of the system, a technical safety concept goes deeper into the technical details of the system. Technical safety requirements are derived from functional safety requirements.

Further, ISO 26262 places the functional safety concept in the concept phase while the technical safety concept is part of the product development phase.

This is because the technical safety concept is more concrete and gets into the details of the item's technology such as sensors, control units and actuators. Technical safety requirements are general hardware and software requirements but still without getting into specific details. For example, in the technical safety concept you might realize that you need to add more ECUs, sensors, and extra software blocks to your system.

So the technical safety concept involves:

- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture
- In addition to mapping from the functional safety requirements, ISO26262 requires technical safety requirements to cover five other categories.
    - Two of the categories are for detecting faults either within the system or in an external device interacting with the system.
    - The other three categories are from measures that enable the system to reach a safe state, to implement a warning and degradation concept, or to prevent latent faults.

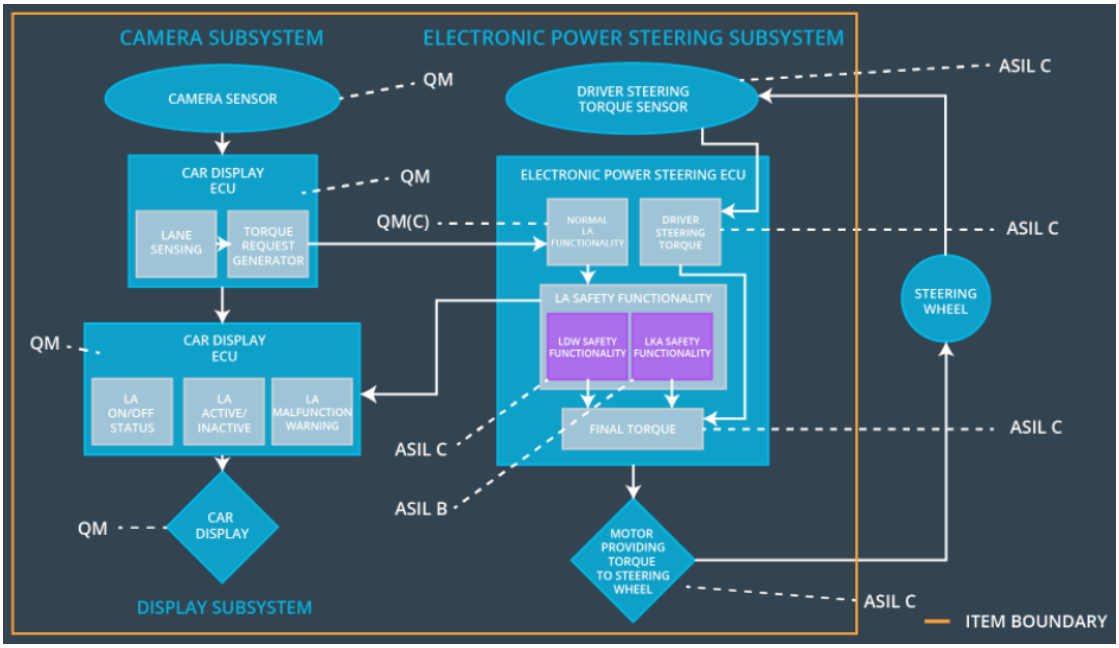
This will help to drill down into software and hardware implementation.

Inputs to the Technical Safety Concept

Functional Safety Requirements

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 01-01	The lane keeping items shall ensure that the lane departure oscillating torque amplitude is below max torque amplitude.	C	50 ms	LDW function will be 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 function will be turned off
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	LKA function will be turned off

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Sensor responsible for capturing vehicle driving conditions such as surrounding vehicles, obstacles and lane lines.
Camera Sensor ECU - Lane Sensing	Software module in the Camera Sensor ECU that is responsible for detecting lane lines and determining ego vehicle's position relative to lane lines.
Camera Sensor ECU - Torque request generator	Software module in the Camera Sensor ECU that is responsible for calculating and sending the additional torque for the LDW and LKA functionality.
Car Display	Visual display warning of lane departures, LDW / LKA activation and deactivations.
Car Display ECU - Lane Assistance On/Off Status	Software module in the Car Display ECU that is responsible for processing information from other item elements and accordingly, decide LDW and LKA ON/OFF status on the car display.
Car Display ECU - Lane Assistant Active/Inactive	Software module in the Car Display ECU that is responsible for processing information from other item elements and accordingly, display warning of lane departures, LDW / LKA activations and deactivations.
Car Display ECU - Lane Assistance malfunction warning	Software module in the Car Display ECU that is responsible for processing information from other item elements and accordingly, display warning of LDW / LKA malfunctions.
Driver Steering Torque Sensor	Sensor responsible for measuring steering torque that the driver is applying on the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Software module in the EPS ECU that is responsible for receiving camera sensor ECU torque requests.
EPS ECU - Normal Lane Assistance Functionality	Software module in the EPS ECU that is responsible for receiving driver steering torque sensor input from the steering wheel.
EPS ECU - Lane Departure Warning Safety Functionality	Software module in the EPS ECU that is responsible for maintaining the lane departure oscillating torque amplitude and frequency values as stated in requirements
EPS ECU - Lane Keeping Assistant Safety Functionality	Software module in the EPS ECU that is responsible for ensuring that LKA torque does not exceed Max_Duration.
EPS ECU - Final Torque	Software module in the EPS ECU that is responsible for ensuring that requests for LDW, LKA are combined before torque request is sent to the actuator.
Motor	Actuator responsible for taking inputs from ECU and then applying requested torque on the steering column

Technical Safety Concept

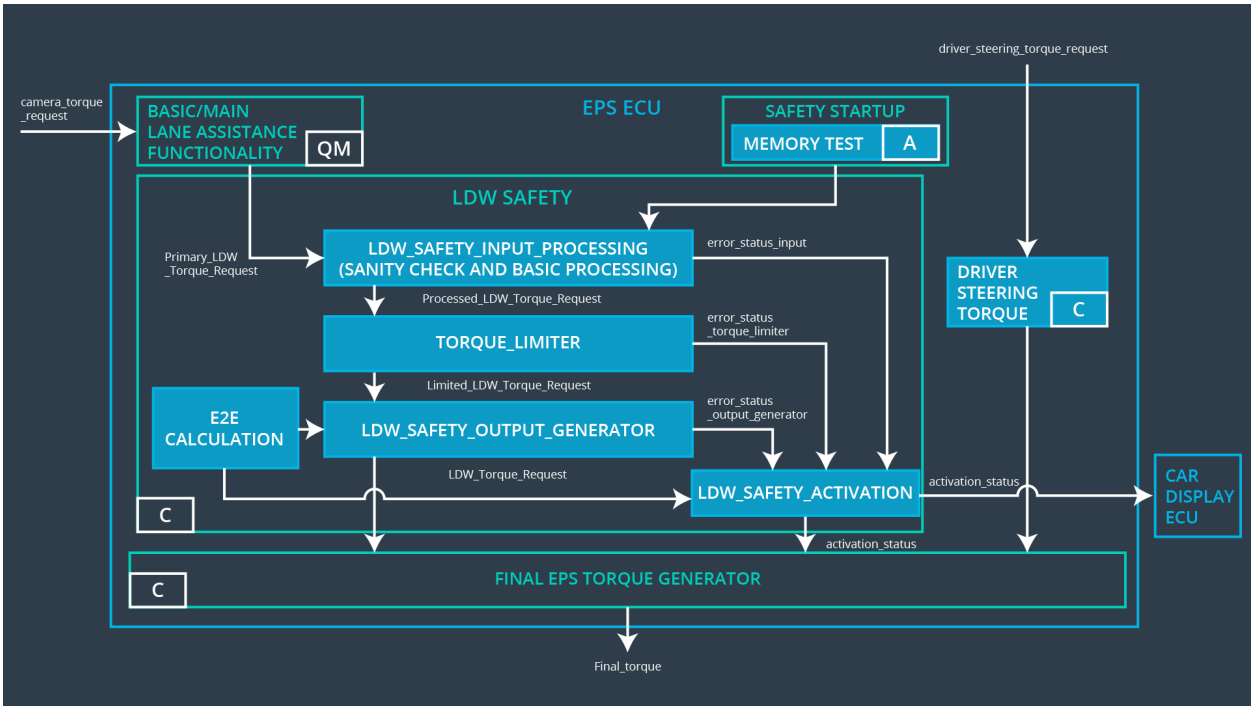
Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements (derived in the functional safety concept)

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		

Technical Safety Requirements related to Functional Safety Requirement 01-01 are:



ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	LDW safety component shall ensure that the amplitude of the ***LDW torque request*** sent to the ***Final Electronic Power Steering Torque*** component is below max torque amplitude.	C	50 ms	LDW safety	The LDW torque request amplitude shall be set to zero.
Technical Safety Requirement 02	The validity and integrity of the data transmission for the ***LDW_Torque_Request*** signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	The LDW torque request amplitude shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ***LDW_Torque_Request*** shall be set to zero.	C	50 ms	LDW safety block	The LDW torque request amplitude shall be set to zero.
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW safety software block shall send a signal to the car display ECU to turn on a warning light.	C	50 ms	LDW safety block	The LDW torque request amplitude shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the start-up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	The LDW torque request amplitude shall be set to zero.

Functional Safety Requirement 01-2 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		

Technical Safety Requirements related to Functional Safety Requirement 01-02 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Architecture Allocation	Safe State
Technical Safety Requirement 01	LDW safety component shall ensure that the frequency of the ***LDW torque request*** sent to the ***Final Electronic Power Steering Torque*** component is below max torque frequency.	C	50 ms	LDW safety	The LDW torque request frequency shall be set to zero.
Technical Safety Requirement 02	The validity and integrity of the data transmission for the ***LDW_Torque_Request*** signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	The LDW torque request frequency shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LDW function, it shall deactivate the LDW feature and the ***LDW_Torque_Request*** shall be set to zero.	C	50 ms	LDW safety block	The LDW torque request frequency shall be set to zero.
Technical Safety Requirement 04	As soon as the LDW function deactivates the LDW feature, the LDW safety software block shall send a signal to the car display ECU to turn on a warning light.	C	50 ms	LDW safety block	The LDW torque request frequency shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the start-up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	The LDW torque request frequency shall be set to zero.

Lane Keeping Assistance (LKA) Requirements:

Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for a duration equal to Max_Duration	X		

Technical Safety Requirements related to Functional Safety Requirement 02-01 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	LKA safety component shall ensure that the ***LKA_Torque_Request*** sent to the ***Final Electronic Power Steering Torque*** component is applied for only Max_duration.	B	500 ms	LKA Safety Component	The LKA torque request shall be set to zero.
Technical Safety Requirement 02	The validity and integrity of the data transmission for the ***LKA_Torque_Request*** signal shall be ensured.	C	500 ms	Data Transmission Integrity Check	The LKA torque request shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall deactivate the LKA feature and the ***LKA_Torque_Request*** shall be set to zero.	B	500 ms	LKA Safety Component	The LKA torque request shall be set to zero.
Technical Safety Requirement 04	As soon as the LKA function deactivates the LKA feature, the LKA safety software block shall send a signal to the car display ECU to turn on a warning light.	B	500 ms	LKA Safety Component	The LKA torque request shall be set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at the start-up of EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	The LKA torque request shall be set to zero.

Refinement of the System Architecture