Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
11/28/18	1.0	Kapy Kangombe	First draft of technical safety concept

Table of Contents

Purpose of the Technical Safety Concept

The purpose of the technical safety concept is to:

- turn functional safety requirements into technical safety requirements, and
- allocate technical safety requirements to the system architecture

The technical safety concept refines the requirements outlined in the functional safety concept and goes into greater detail by drilling down into the relevant subsystems (i.e., focusing on component level).

However, not all technical safety requirements are derived from functional safety requirements. ISO 26262 requires five other categories of technical safety requirements:

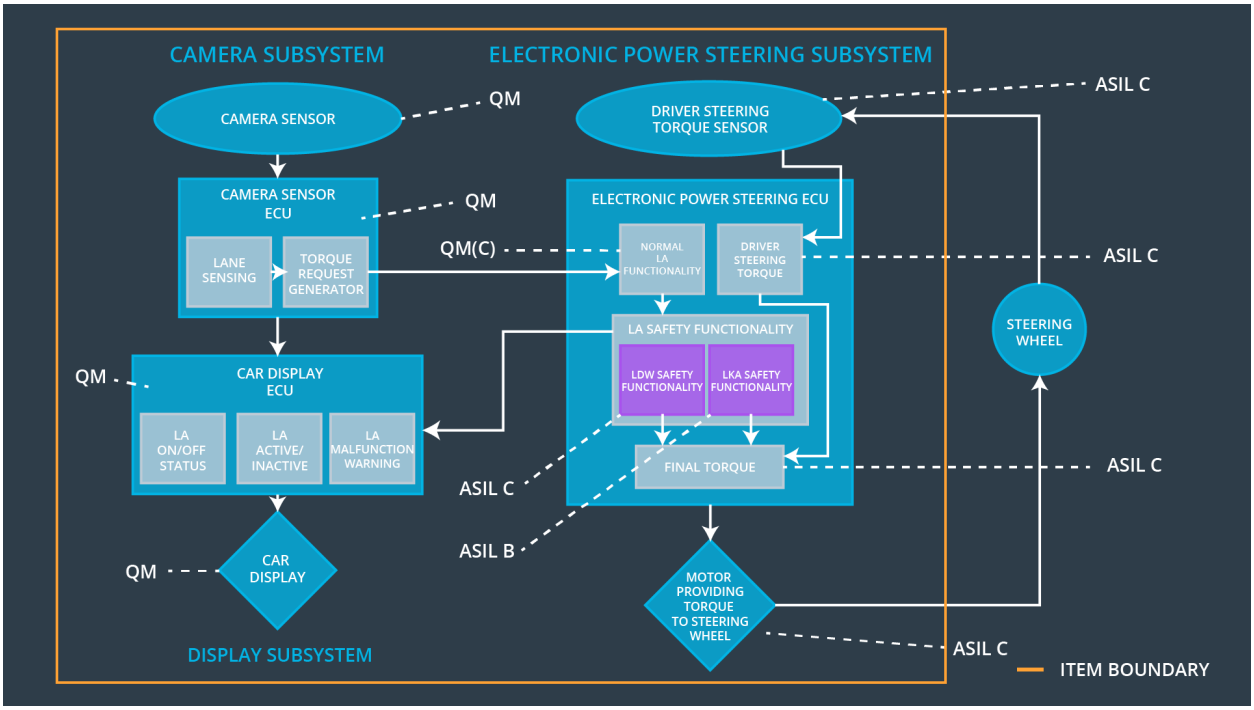
1. Detecting faults within a system
2. Detecting faults in an external device interacting with the system
3. Reaching a safe state
4. Implementing a warning and degradation concept
5. Preventing latent faults

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 electronic power steering ECU shall ensure that the lane departure warning oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	LDW function turned off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure warning oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	LDW function turned off
Functional Safety Requirement 02-01	Electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only Max_Duration	B	500 ms	LKA function turned off

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	A sensor that detects lane departures.
Camera Sensor ECU - Lane Sensing	A software block that senses where the vehicle is with respect to the lane (i.e., lane departure detection).
Camera Sensor ECU - Torque request generator	A software block to send a torque to the electronic power steering ECU subsystem.
Car Display	A screen that displays a warning of the vehicle lane departure to the driver and also shows the status (on/off) of the the lane keeping function.
Car Display ECU - Lane Assistance On/Off Status	A software block that controls a light that tells the driver if the lane keeping item is on or off.
Car Display ECU - Lane Assistant Active/Inactive	A software block that controls a light that tells the driver if the lane departure warning is activated.
Car Display ECU - Lane Assistance malfunction warning	A component that displays warning lights/information when there is a malfunction message sent from the electronic power steering ECU.
Driver Steering Torque Sensor	A component that senses how much the driver is turning the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	A software block to analyze the driver steering torque from the driver steering torque sensor.
EPS ECU - Normal Lane Assistance Functionality	A software block that receives the vibrational torque request from the camera subsystem. It takes care of normal functional behavior.
EPS ECU - Lane Departure Warning Safety Functionality	A software block that takes care of LDW malfunctions and applies oscillating torque amplitude & frequency limits.
EPS ECU - Lane Keeping Assistant Safety Functionality	A software block that takes care of LKA malfunctions and applies the max_duration limits.
EPS ECU - Final Torque	The component that adds the torque request from the camera subsystem and driver steering torque.
Motor	Provides torque to the steering wheel to help the driver move the vehicle back towards the center of the lane.

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	The 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	Lane Departure Warning Safety block	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Departure Warning 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	Lane Departure Warning 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	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup (Memory Test)	Lane Departure Warning 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	The 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 block	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Departure Warning 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	Lane Departure Warning 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	Lane Departure Warning Torque Request Amplitude shall be set to zero
Technical	Memory test shall be conducted at	A	Ignition	Safety Startup	Lane

Safety Requirement 05	start up of the EPS ECU to check for any faults in memory.		cycle	(Memory Test)	Departure Warning Torque Request Amplitude shall be set to zero

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:
N/A (optional)

Lane Keeping Assistance (LKA) Requirements:

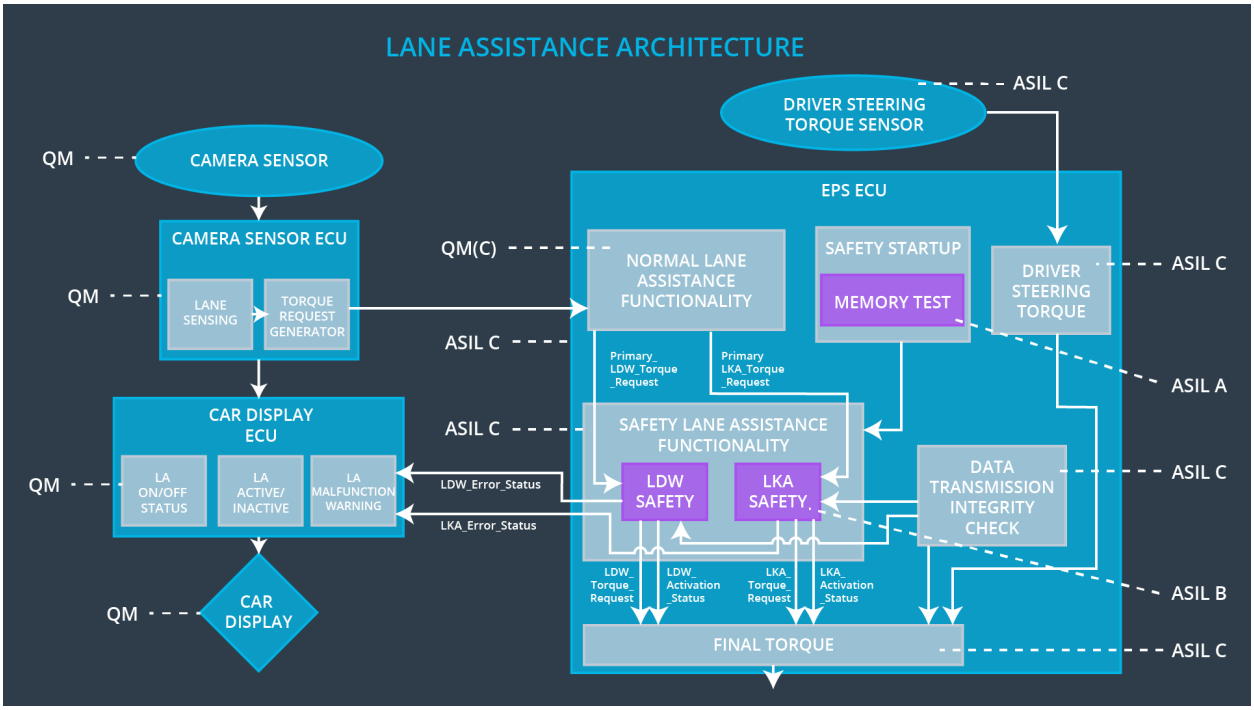
Functional Safety Requirement 02-1 with its associated system elements (derived in the functional safety concept)

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 only 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	The LKA safety component shall ensure that 'LKA_Torque_Request' is sent to the 'Final electronic power steering Torque' component for only Max_Duration.	B	500 ms	LKA Safety block	Lane Keeping Assistance Torque Request Amplitude shall be set to zero
Technical Safety Requirement 02	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	Lane Keeping Assistance Torque Request Amplitude 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 block	Lane Keeping Assistance Torque Request Amplitude 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 block	Lane Keeping Assistance Torque Request Amplitude shall be set to zero
Technical Safety Requirement 05	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Safety Startup (Memory Test)	Lane Keeping Assistance Torque Request Amplitude shall be set to zero

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

For this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW function	LDW malfunction	Yes	LDW malfunction warning light on dashboard
WDC-02	Turn off LKA function	LKA malfuntion	Yes	LKA malfunction warning light on dashboard