Technical Safety Concept Lane Assistance

Document Version: 1.0, Released on 2017-12-26

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
2017/12/26	1.0	Daniel Prado	Initial Version

Table of Contents

Document history

Table of Contents

Purpose of the Technical Safety Concept

Inputs to the Technical Safety Concept
- Functional Safety Requirements
- Refined System Architecture from Functional Safety Concept
  - Functional overview of architecture elements

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

Purpose of the Technical Safety Concept

The creation of a technical safety concept is part of the safety process of ISO 26262 for the treatment of potential malfunctions in electrical and electronic systems.

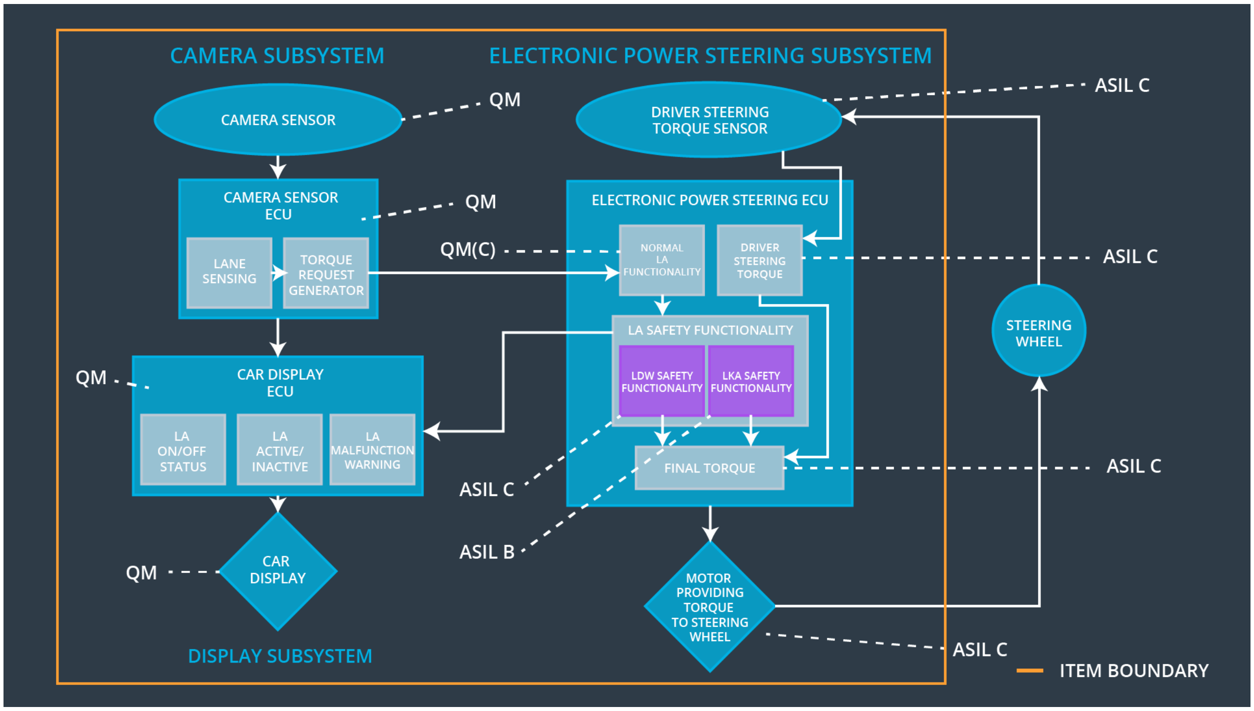
Its purpose is to transform functional safety requirements into additional (more detailed) technical requirements and allocate these high-level hardware and software requirements to the system arquitecture.

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 item shall ensure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude.	C	50ms	Torque 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	50ms	Torque set to zero.
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	500ms	LKA disengaged and extra torque = zero.

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Sensor for the optical detection of the front area of the vehicle, including detectable lane lines.
Camera Sensor ECU - Lane Sensing	Lane Sensing module (part of Camera Sensor ECU) is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake. Pass information to the ‘Torque Request Generator’ module of the same ECU.
Camera Sensor ECU - Torque request generator	Torque request generator module (part of Camera Sensor ECU) is responsible for calculating and sending request for additional steering torque to the Electronic Power Steering ECU.
Car Display	Visual display which is, among other functionalities, responsible for displaying warning of lane departures and displaying LKA and LDW status.

Car Display ECU - Lane Assistance On/Off Status	Component in the Car Display ECU responsible for controlling the display indicator for Lane Assistance system status ON or OFF.
Car Display ECU - Lane Assistant Active/Inactive	Component in the Car Display ECU responsible for controlling the display indicator to show activation of the LKA or LDW functions to the driver.
Car Display ECU - Lane Assistance malfunction warning	Component in the Car Display ECU responsible for controlling the display indicator that shows any malfunction within the lane assistance system.
Driver Steering Torque Sensor	Sensor responsible for measuring the steering torque provided by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Component in the EPS ECU that receives and process the signal of the driver steering torque sensor processes it, and passes the result to the Final Torque module.
EPS ECU - Normal Lane Assistance Functionality	Component in the EPS ECU that receives and processes the extra torque request from the camera sensor ECU and calculates the assistance torque according to the input.
EPS ECU - Lane Departure Warning Safety Functionality	Component in the EPS ECU responsible for keeping the lane departure warning action (oscillating torque) below Max_Torque_Amplitude and Max_Torque_Frequency. The component is also responsible for ensuring that the lane departure warning is only applied when LDW_On is set.
EPS ECU - Lane Keeping Assistant Safety Functionality	Component within the EPS ECU responsible for ensuring that the lane keeping assistance is not forcing the car longer than Max_Duration to the center of the lane.
EPS ECU - Final Torque	Component within the EPS ECU responsible for ensuring that the single torque values from LDW, LKA are combined with the drivers original steering torque and sent to the motor.
Motor	Device that adds extra torque to the steering wheel.

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	50ms	EPS ECU - LDW Safety Component	LDW torque output is set to zero.
Technical Safety Requirement 02	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	50ms	EPS ECU - LDW Safety Component	LDW torque output is 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	50ms	EPS ECU - LDW Safety Component	LDW torque output is set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50ms	EPS ECU – Data Transmission Integrity Check	LDW torque output is set to zero.
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup Memory Test	LDW torque output is 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 amplitude of the 'LDW_Torque_Request' sent to the 'Final electronic power steering Torque' component is below 'Max_Torque_Frequency.	C	50 ms	EPS ECU - LDW Safety Component	Torque Freq. below maximum

Technical Safety Requirement 02	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	EPS ECU - LDW Safety Component	N/A
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	EPS LDW Safety Software Component	Torque set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LDW_Torque_Request' signal shall be ensured.	C	50 ms	EPS ECU - Data Transmission Integrity Check	N/A
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	N/A

Lane Keeping Assistance (LKA) Requirements:

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

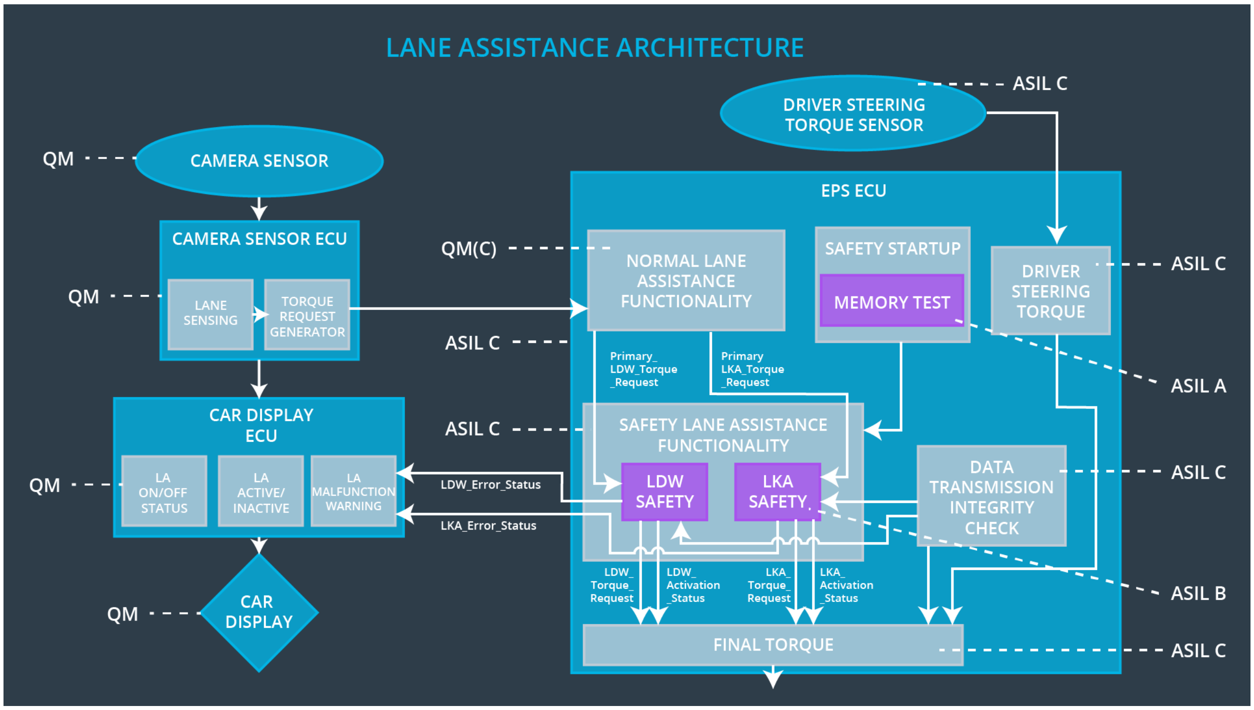
ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane keeping assistance torque is applied for only Max_Duration	X		

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 the duration of the lane keeping assistance torque applied is less than Max_Duration.	C	500ms	EPS ECU - LKA Safety Component	LKA disengages , Set the lane keeping extra torque to zero.
Technical Safety Requirement 02	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.	C	500ms	EPS ECU - LKA Safety Component	N/A
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.	C	500ms	EPS ECU - LKA Safety Component	Torque set to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	C	500ms	EPS ECU – Data Transmission Integrity Check	N/A
Technical Safety Requirement 05	Memory test shall be conducted at startup of the EPS ECU to check for any faults in memory.	A	Ignition cycle	EPS ECU – Safety Startup	N/A

Refinement of the System Architecture

The following images shows the refined system architecture:



Allocation of Technical Safety Requirements to Architecture Elements

All technical safety requirements detailed in this document are allocated to the Electronic Power Steering ECU, as already stated above in the technical requirement tables.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Turn off LDW functionality	Vibration amplitude too high (+/- 3 N-m) or frequency too high.	Yes, LDW oscillating torque shall be set to zero	Lane assistance functionality set inactive and malfunction warning to the driver via car display.
WDC-02	Turn off LKA functionality	Lane keeping assistance duration exceeds Max_Duration	Yes, LKA added extra torque shall be set to zero	Lane assistance functionality set inactive and malfunction warning to the driver via car display.