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
2017-06-13	1.0	Markus Isaksson	First attempt

Table of Contents

Purpose of the Technical Safety Concept

The Technical Safety Concept refines the Functional Safety Requirements into more technical details to include the signal flow and which components are in charge of the functionality. Note that components are elements in a system, so where the Functional Safety Concept allocated requirements to subsystems, the Technical Safety Concept delves further into the architecture and allocates requirements to components in those subsystems. The Technical Safety Concept also identifies requirements that not are directly related to Functional Safety Requirements, such as requirements dealing with internal or external communication faults, latent memory errors etc.

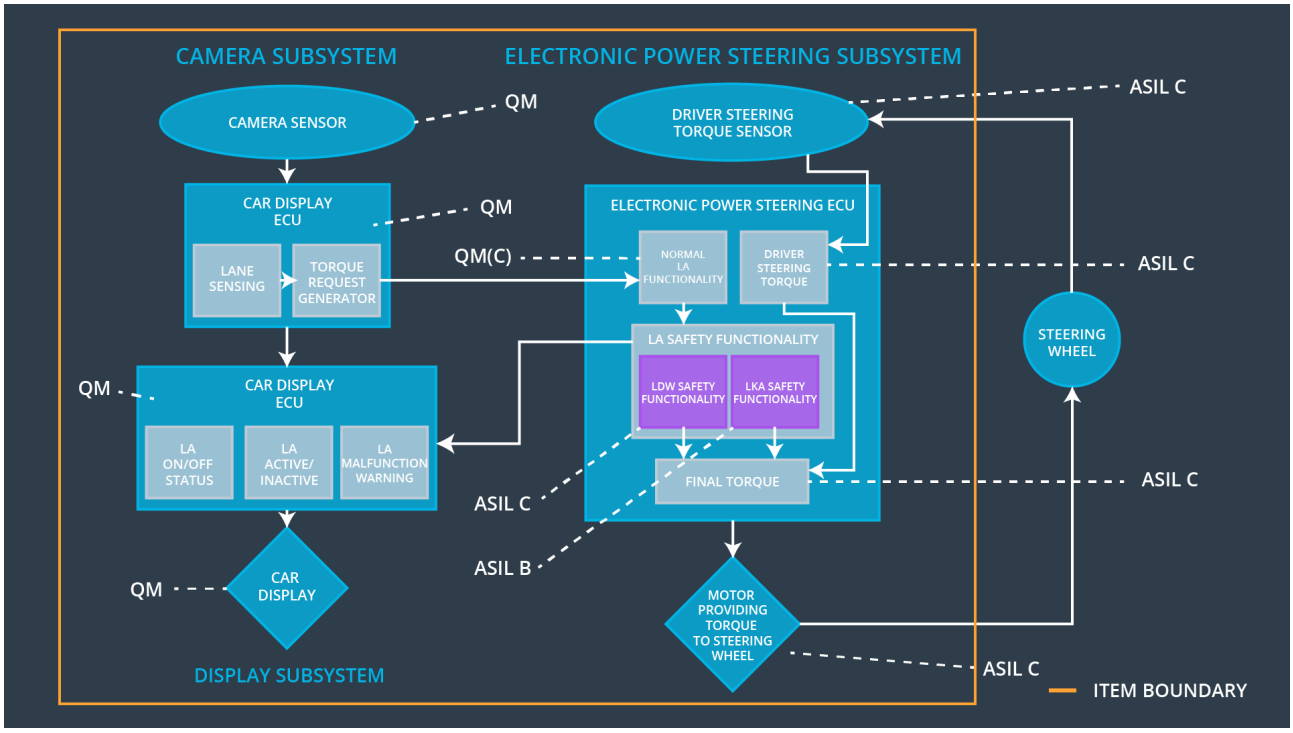
A safety case typically have multiple levels of Technical Safety Concepts, with one document for each subsystem that have safety relevance. In this fictive Lane Assistance project, all safety relevant parts are allocated to the Electronic Power Steering ECU; thus, only one document will be produced for this project.

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 oscillating torque amplitude is below Max_Torque_Amplitude	C	50 ms	Lane Assistance is turned off
Functional Safety Requirement 01-02	The electronic power steering ECU shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	C	50 ms	Lane Assistance is 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 is deactivated
Functional Safety Requirement 02-02	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Lane_Keep_Torque.	B	50 ms	Lane Assistance is turned off
Functional Safety Requirement 02-03	The electronic power steering ECU shall ensure that the lane keeping assistance applies no torque when the driver steering torque exceeds Max_Drifting_Torque.	A	50 ms	LKA is deactivated

Refined System Architecture from Functional Safety Concept



Functional overview of architecture elements

Element	Description
Camera Sensor	Forward looking camera capturing images of the road ahead of ego vehicle.
Camera Sensor ECU - Lane Sensing	Detects lane lines in the Camera Sensor images.
Camera Sensor ECU - Torque request generator	Determines when the vehicle leaves the lane by mistake and then generate torque requests for both the LDW and LKA functions.
Car Display	Display mounted in the vehicle dashboard to present information to the driver.
Car Display ECU - Lane Assistance On/Off Status	Draws a symbol on the Car Display indicating if the Lane Assitant is on or off.
Car Display ECU - Lane Assistant Active/Inactive	Draws a symbol on the Car Display indicating if the Lane Assistant is active or inactive.
Car Display ECU - Lane Assistance malfunction warning	Draws a symbol on the Car Display indicating if the Lane Assistant have a malfunction.
Driver Steering Torque Sensor	Measures the torque applied on the steering wheel by the driver.

Electronic Power Steering (EPS) ECU - Driver Steering Torque	Reads the Driver Steering Torque Sensor.
EPS ECU - Normal Lane Assistance Functionality	Interfaces the Camera Sensor ECU’s requests of torque to apply for normal Lane Assistance functionality.
EPS ECU - Lane Departure Warning Safety Functionality	Detects and deals with malfunctions in the LDW torque requests.
EPS ECU - Lane Keeping Assistant Safety Functionality	Detects and deals with malfunctions in the LKA torque requests.
EPS ECU - Final Torque	Calculates the actual torque to apply on the steering wheel by this item. Interfaces the Motor.
Motor	Steering wheel torque actuator.

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 electronic power steering ECU 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 Torque’ component is below Max_Torque_Amplitude.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 02	When a failure is detected by the ‘LDW Safety’ component, this shall be indicated in the LDW_Torque_Request signal.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 03	When the ‘Final Torque’ component receives a LDW_Torque_Request signal indicating a failure, then it shall set LA_Final_Torque to zero.	C	50 ms	Final Torque	Lane Assistance is turned off
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Assistance is turned off
Technical Safety Requirement 05	When a failure is detected by the ‘LDW Safety’ component,this shall be indicated in the LDW_Error_Status signal.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 06	When the ‘LA Malfunction Warning’ component receives a LDW_Error_Status signal indicating a failure, then it shall draw a symbol on the Car Display indicating that the LA item is turned of due to a malfunction.	QM	50 ms	LA Malfunction Warning	Lane Assistance is turned off
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	Lane Assistance is turned off

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 electronic power steering ECU 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 Torque’ component is below Max_Torque_Frequency.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 02	When a failure is detected by the ‘LDW Safety’ component, this shall be indicated in the LDW_Torque_Request signal.	C	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 03	When the ‘Final Torque’ component receives a LDW_Torque_Request signal indicating a failure, then it shall set LA_Final_Torque to zero.	C	50 ms	Final Torque	Lane Assistance is turned off
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LDW_Torque_Request’ signal shall be ensured.	C	50 ms	Data Transmission Integrity Check	Lane Assistance is turned off
Technical Safety Requirement 05	When a failure is detected by the ‘LDW Safety’ component,this shall be indicated in the LDW_Error_Status signal.	C	50 ms	LDW Safety	Lane Assistance is turned off

Technical Safety Requirement 06	When the ‘LA Malfunction Warning’ component receives a LDW_Error_Status signal indicating a failure, then it shall draw a symbol on the Car Display indicating that the LA item is turned of due to a malfunction.	QM	50 ms	LA Malfunction Warning	Lane Assistance is turned off
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	Lane Assistance is turned off

Lane Departure Warning (LDW) Verification and Validation Acceptance Criteria:
TBD

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 electronic power steering ECU 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 that the LKA_Torque_Request signal is continuously non-zero is limited to Max_Duration, by then forcing the LKA_Torque_Request signal to zero for a duration of LKA_Deactivation_Period.	B	500 ms	LKA Safety	LKA function is deactivated

Technical Safety Requirement 02	When the ‘LKA Safety’ component forces the LKA_Torque_Request signal to zero, this shall be indicated by the LKA_Error_Status signal.	B	500 ms	LKA Safety	LKA function is deactivated
Technical Safety Requirement 03	When the ‘LA Malfunction Warning’ component receives a LKA_Error_Status signal indicating that the LKA_Torque_Request signal is forced to zero, then it shall draw a symbol on the Car Display indicating that LKA is deactivated.	QM	500 ms	LA Malfunction Warning	LKA function is deactivated
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured.	B	500 ms	Data Transmission Integrity Check	Lane Assistance is turned off
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	Memory Test	Lane Assistance is turned off

Functional Safety Requirement 02-2 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 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is below Max_Lane_Keep_Torque	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 LKA_Torque_Request signal is below Max_Lane_Keep_Torque.	B	50 ms	LDW Safety	Lane Assistance is turned off

Technical Safety Requirement 02	When a failure is detected by the ‘LKA Safety’ component, this shall be indicated in the LKA_Torque_Request signal.	B	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 03	When the ‘Final Torque’ component receives a LKA_Torque_Request signal indicating a failure, then it shall set LA_Final_Torque to zero.	B	50 ms	Final Torque	Lane Assistance is turned off
Technical Safety Requirement 04	The validity and integrity of the data transmission for ‘LKA_Torque_Request’ signal shall be ensured.	B	50 ms	Data Transmission Integrity Check	Lane Assistance is turned off
Technical Safety Requirement 05	When a failure is detected by the ‘LKA Safety’ component, this shall be indicated in the LKA_Error_Status signal.	B	50 ms	LDW Safety	Lane Assistance is turned off
Technical Safety Requirement 06	When the ‘LA Malfunction Warning’ component receives a LKA_Error_Status signal indicating a failure, then it shall draw a symbol on the Car Display indicating that the LA item is turned of due to a malfunction.	QM	50 ms	LA Malfunction Warning	Lane Assistance is turned off
Technical Safety Requirement 07	Memory test shall be conducted at start up of the EPS ECU to check for any faults in memory.	A	Ignition cycle	Memory Test	Lane Assistance is turned off

Functional Safety Requirement 02-2 with its associated system elements (derived in the functional safety concept)

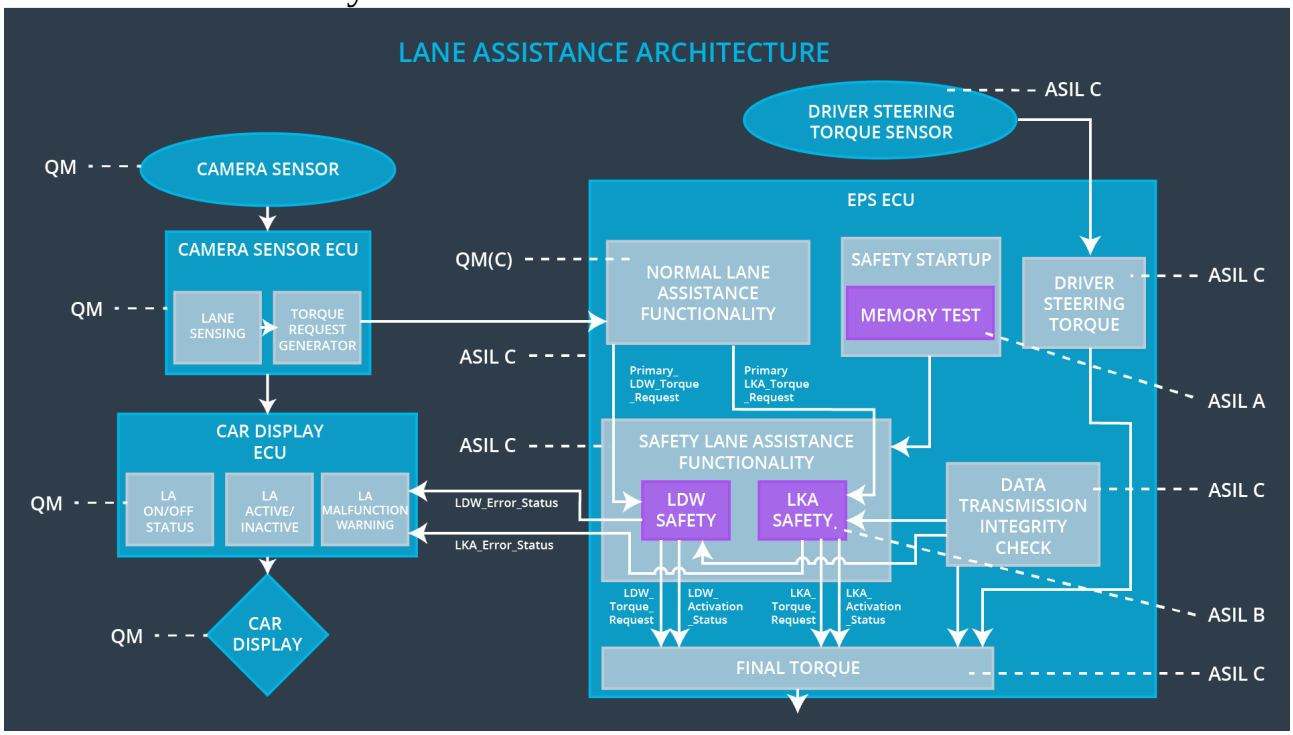
ID	**Functional Safety Requirement**	**Electronic Power Steering ECU**	**Camera ECU**	**Car Display ECU**
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance applies no torque when the driver steering torque exceeds Max_Drifting_Torque.	X		

Technical Safety Requirements related to Functional Safety Requirement 02-03 are:

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The ‘LKA Safety’ component shall detect when the Driver_Steering_Torque signal is above Max_Drifting_Torque and if so, force the LKA_Torque_Request signal to zero for a duration of LKA_Deactivation_Period.	A	50 ms	LKA Safety	LKA function is deactivated
Technical Safety Requirement 02	When the ‘LKA Safety’ component forces the LKA_Torque_Request signal to zero, this shall be indicated by the LKA_Error_Status signal.	A	50 ms	LKA Safety	LKA function is deactivated
Technical Safety Requirement 03	When the ‘LA Malfunction Warning’ component receives a LKA_Error_Status signal indicating that the LKA_Torque_Request signal is forced to zero, then it shall draw a symbol on the Car Display indicating that LKA is deactivated.	QM	50 ms	LA Malfunction Warning	LKA function is deactivated
Technical Safety Requirement 04	The validity and integrity of the data transmission for LKA_Torque_Request signal shall be ensured.	A	50 ms	Data Transmission Integrity Check	Lane Assistance is turned off
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	Memory Test	Lane Assistance is turned off

Lane Keeping Assistance (LKA) Verification and Validation Acceptance Criteria:
TBD

Refinement of the System Architecture



Allocation of Technical Safety Requirements to Architecture Elements

This allocation is part of the technical requirement tables. Note that all Technical Safety Requirements that have ASIL A or higher are allocated to components of the Electronic Power Steering ECU.

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Lane Assistance turned off until the vehicle is restarted.	Malfunction_01 Malfunction_02 Malfunction_04	Yes	Activate a warning symbol on Car Display indicating that the Lane Assistance item has been turned off.
WDC-02	LKA is deactivated for a duration of LKA_Deactivation_Period.	Malfunction_03	Yes	1. Activate a warning symbol on the Car Display indicating that LKA is deactivated. 2. Sound an alarm signal.
WDC-03	LKA is deactivated for a duration of LKA_Deactivation_Period, measured from the most recent triggering.	Malfunction_05	Yes	Activate a warning symbol on the Car Display indicating that LKA is deactivated.