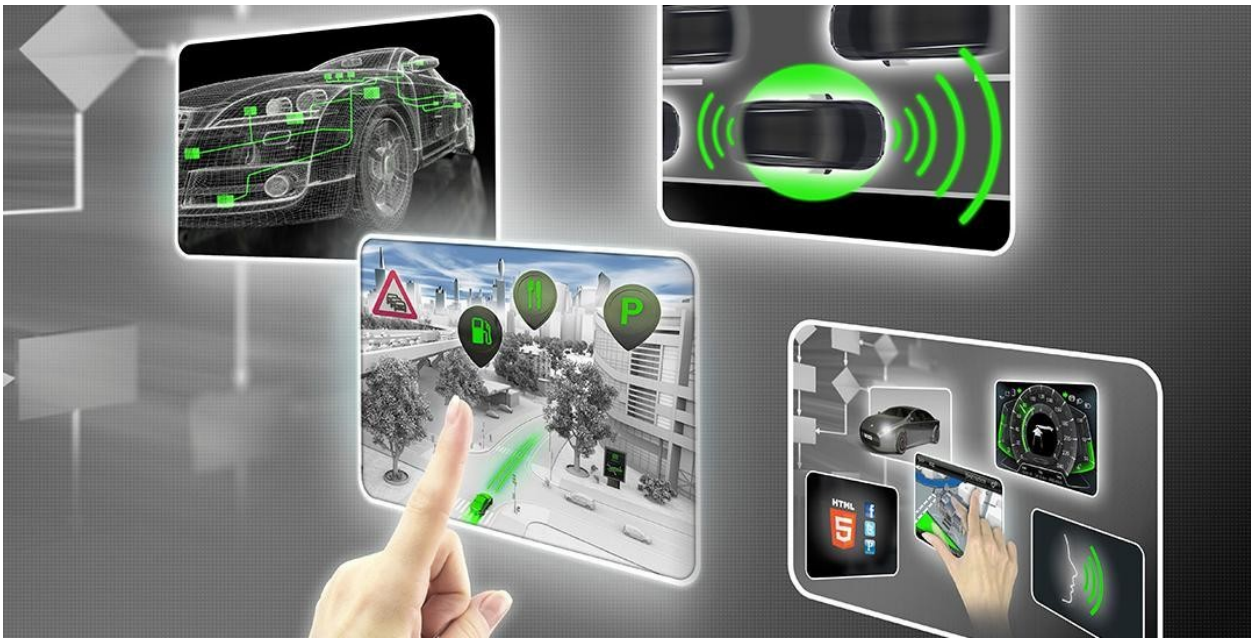
Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Purpose of the Technical Safety Concept

[Instructions: Answer what is the purpose of a technical safety concept?]

The purpose of the Technical Safety Concept is to translates high-level functional safety requirements into functional safety requirements based on the system architecture.

Inputs to the Technical Safety Concept

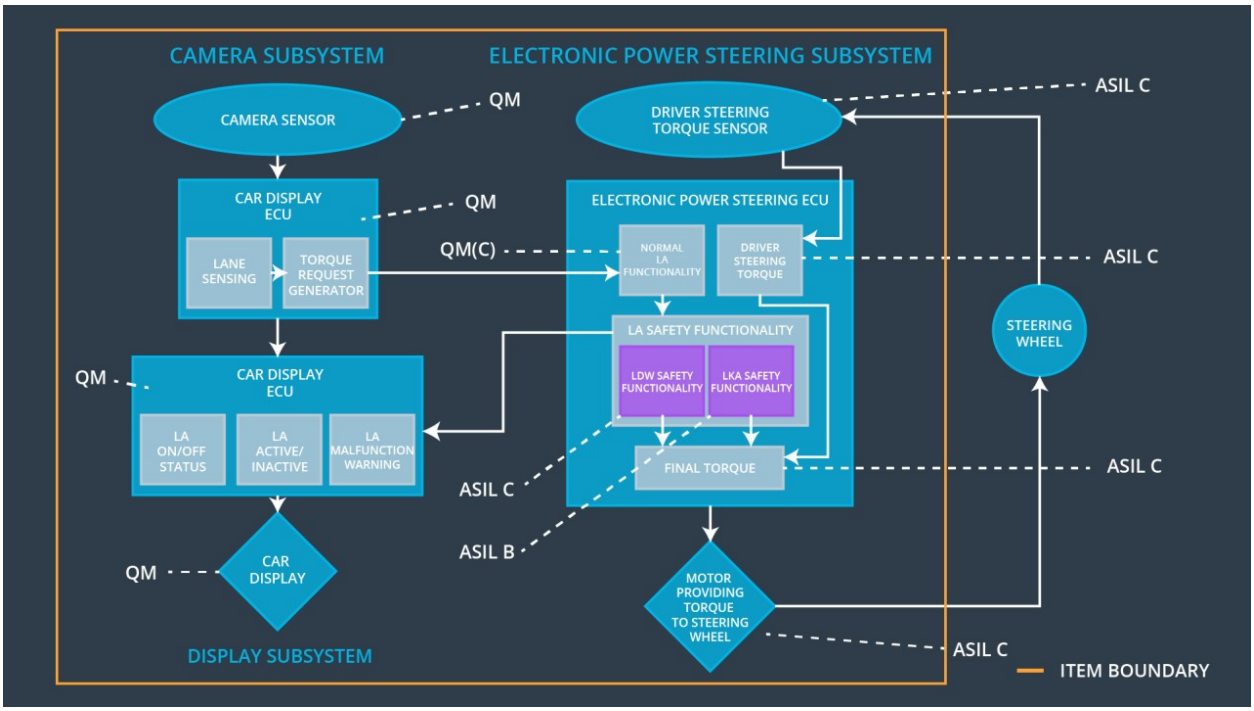
Functional Safety Requirements

[Instructions: Provide the functional safety requirements derived in the functional safety concept]

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 oscillating torque amplitude requested by the LDW function is below Max_Torque_Amplitude.	C	50 ms	The Lane Assistance functionality is switched 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	The Lane Assistance functionality is switched off.
Functional Safety Requirement 02-01	The lane keeping item shall ensure that the lane departure oscillating torque frequency is above Min_Torque_Frequency.	B	50 ms	The Lane Assistance functionality is switched off.

Refined System Architecture from Functional Safety Concept

[Instructions: Provide the refined system architecture from the functional safety concept]



Functional overview of architecture elements

[Instructions: Provide a description for each functional safety element; what is each element's purpose in the lane assistance item?]

Element	Description
Camera Sensor	The Camera Sensor reads in images from the road.
Camera Sensor ECU - Lane Sensing	Lane Sensing element process the images from Cmaera Sensor to identifies when the vehicle is leaving the lane.
Camera Sensor ECU - Torque request generator	The Camera Sensor ECU Torque Request Generator determine necessary torque for lane keeping and sends signals to Electronic Power Steering ECU and Car Display ECU.
Car Display	The Car Display shows the current status of LDW and LK functions by turning on/off status lights.
Car Display ECU - Lane Assistance On/Off Status	Lane Assistance On/Off Status element sends a signal to the Car Display to notify whether each LA function has been turned on or off.
Car Display ECU - Lane Assistant Active/Inactive	Lane Assistant Active/Inactive element sends a signal to the Car Display to turn on the Lane Assistance Active status light. The Car Display ECU LA Active/Inactive element determines whether the lane assist is active or inactive for display on the dashboard.
Car Display ECU - Lane Assistance malfunction warning	The Car Display ECU LA Malfunction Warning element receives LDW_Error_Status messages and provides appropriate warnings on the display.
Driver Steering Torque Sensor	The Driver Steering Torque Sensor detects the amount of torque from the steering wheel.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Driver Steering Torque element sends a signal from the Driver Steering Torque Sensor to the Final Torque element with the amount of torque applied by the driver.
EPS ECU - Normal Lane Assistance Functionality	Normal Lane Assistance Functionality element sends messages from Torque Request Generator to Lane Assistance Safety module.

EPS ECU - Lane Departure Warning Safety Functionality	Lane Departure Warning Safety Functionality element ensures that the LDW functionality does not malfunction.
EPS ECU - Lane Keeping Assistant Safety Functionality	Lane Keeping Assistant Safety Functionality element is responsible for safety-related functions.
EPS ECU - Final Torque	Final Torque element combines signals from Lane Assistance Safety module and Driver Steering Torque module
Motor	The Motor provides torque for the steering wheel.

Technical Safety Concept

Technical Safety Requirements

[Instructions: Fill in the technical safety requirements for the lane departure warning first functional safety requirement. We have provided the associated functional safety requirement in the first table below. Hint: The technical safety requirements were discussed in the lesson videos. The architecture allocation column should contain element names such as LDW Safety block, Data Transmission Integrity Check, etc. Allocating the technical safety requirements to the "EPS ECU" does not provide enough detail for a technical safety concept.]

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	LDW safety	The LDW torque amplitude is set to 0
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	LDW safety	The LDW torque amplitude is set to 0
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	The LDW torque amplitude is set to 0
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	The LDW torque amplitude is set to 0
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	The LDW torque amplitude is set to 0

[Instructions: Fill in the technical safety requirements for the lane departure warning second functional safety requirement. We have provided the associated functional safety requirement in the table below. Hint:. Most of the technical safety requirements will be the same. At least one technical safety requirement will have to be slightly modified because we are talking about frequency instead of amplitude. These requirements were not given in the lessons]

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	The LDW torque frequency is set to 0
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	LDW Safety	The LDW torque frequency is set to 0
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	The LDW torque frequency is set to 0
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	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	The LDW torque frequency is set to 0

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Lane Keeping Assistance (LKA) Requirements:

[Instructions: Fill in the technical safety requirements for the lane keeping assistance functional safety requirement 02-01. We have provided the associated functional safety requirement in the table below. Hint:. You can reuse the technical safety requirements from functional safety requirement 01-01. But you need to change the language because we are now looking at a different system. The ASIL and Fault Tolerant Time Interval are different as well.]

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:

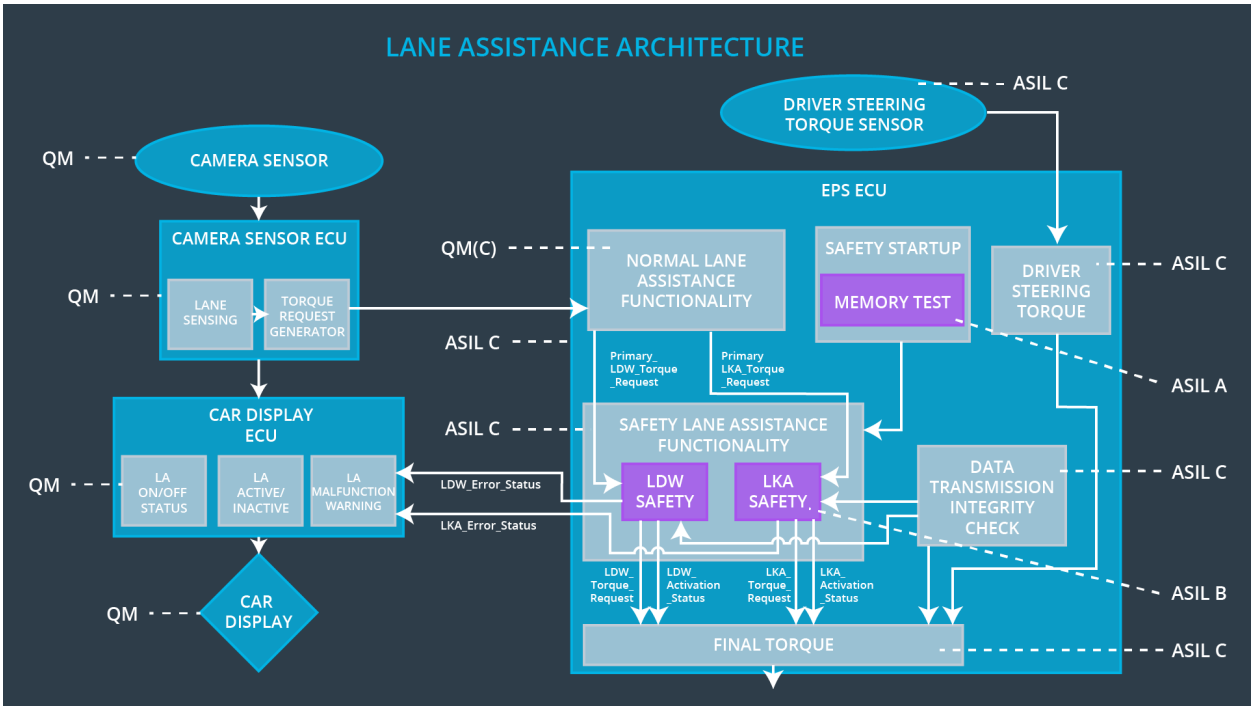
ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 01	The LKA safety component shall make sure that the duration of LK usage is less than Max_Duration.	B	500 ms	LKA Safety	The LKA system will completely turn off
Technical Safety Requirement 02	As soon as the LKA function deactivates the LKA feature, the 'LKA Safety' software block shall notify the car display ECU to turn on a warning light.	B	500 ms	LKA Safety	The LKA system will completely turn off
Technical Safety Requirement 03	As soon as a failure is detected by the LKA function, it shall turn off the LKA feature and the 'LKA_Torque_Request' shall be set to 0.	B	500 ms	LKA Safety	The LKA system will completely turn off
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	The LKA system will completely turn off
Technical Safety Requirement 05	Memory test shall be conducted to check for any faults in memory during the start up of the EPS ECU.	A	Ignition Cycle	Safety Startup	The LKA system will completely turn off

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

[OPTIONAL: For each technical safety requirement, identify both the verification and validation acceptance criteria. “Validation” asks whether or not you chose the appropriate parameters. “Verification” involves testing to make sure the vehicle behaves as expected when the parameter value is crossed. There is not necessarily one right answer. Look at your verification and validation acceptance criteria from the functional safety concept for inspiration.]

Refinement of the System Architecture

[Instructions: Include the refined system architecture. Hint: The refined system architecture should include the system architecture from the end of the technical safety lesson, including all of the ASIL labels.]



Allocation of Technical Safety Requirements to Architecture Elements

[Instructions: We already included the allocation as part of the technical requirement tables. Here you can state that for this particular item, all technical safety requirements are allocated to the Electronic Power Steering ECU]

All technical safety requirements are allocated to the electronic power steering ECU.

Warning and Degradation Concept

[Instructions: We've already identified that for any system malfunction, the lane assistance functions will be turned off and the driver will receive a warning light indication. The technical safety requirements have not changed how functionality will be degraded or what the warning will be.

So in this case, the warning and degradation concept is the same for the technical safety requirements as for the functional safety requirements. You can copy the functional safety warning and degradation concept here.

Oftentimes, a technical safety analysis will lead to a more detailed warning and degradation concept.]

ID	Mode	Degradation Mode	invoked?	Driver Warning
WDC-01	Turn off the functionality	The amplitude of oscillating torque from LDW is greater than Max_Torque_Amplitude	Yes	Display warning light
WDC-02	Turn off the functionality	The frequency of oscillating torque from LDW is greater than Max_Torque_Frequency	Yes	Display warning light
WDC-03	Turn off the functionality	The frequency of oscillating torque from LDW is less than Min_Torque_Frequency	Yes	Display warning light