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
15.11.2018	1.0	Suraj Lal Putta	Initial draft

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

ISO 26262 places the functional safety concept in the concept phase while the technical safety concept is part of the product development phase. The technical safety concept is more concrete and gets into the details of the item's technology. The product development phase is divided into two parts product development at the system level and product development at the hardware and software level. Before developing hardware or software, the technical safety requirements need to be determined for each of these systems. The technical safety concept involves:

- Turning functional safety requirements into technical safety requirements
- Allocating technical safety requirements to the system architecture

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 assistance item shall ensure that the lane departure oscillating torque amplitude is below “Max_Torque_Amplitude”.	C	50ms	The lane departure warning (LDW) function is turned off.
Functional Safety Requirement 01-02	The lane assistance item shall ensure that the lane departure oscillating torque frequency is below “Max_Torque_Frequency”.	C	50ms	The lane departure warning function 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	500ms	The lane keeping assistance (LKA) function is turned off.

Refined System Architecture from Functional Safety Concept

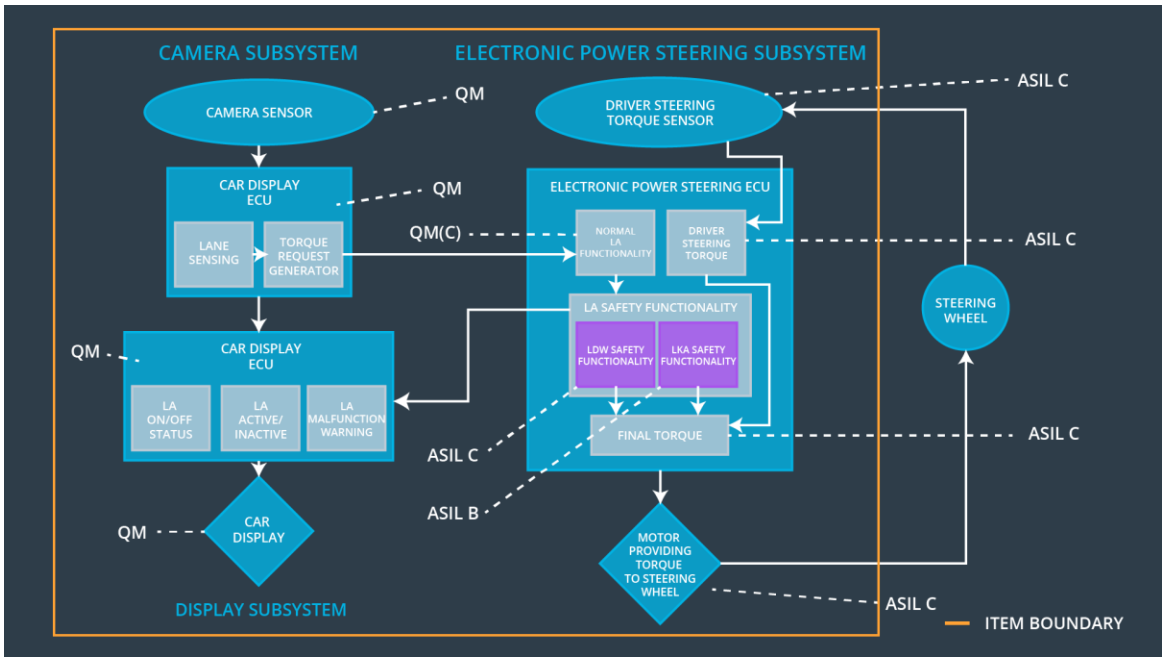

Figure 1: Refined Architecture of the Lane Assistance Item

The refined architecture of the lane assistance item derived from functional safety concept is shown in the picture Figure 1. The picture shows the components of the sub-systems of the lane assistance item. Their ASIL levels already allotted to the components from the functional safety concept. Now the technical safety concept takes the functional safety requirements and derives technical safety requirements and allots them the different components. There are additional technical safety requirements which are not directly derived from functional safety requirements. ISO26262 requires the following categories for additional technical safety requirements. They are also defined here.

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 captures the image of the road ahead which the camera sensor ECU processes it.
Camera Sensor ECU - Lane Sensing	The lane sensing element of the camera sensor ECU processes the captured image and calculates the position of lanes and the ego vehicle.
Camera Sensor ECU - Torque request generator	The torque request generator part of the camera

	sensor ECU receives the lane and ego vehicle positions. Based on this information it calculates the oscillating steering torque for the LDW function and the supporting steering torque for the LKA function. The torque request is then sent to the power steering ECU.
Car Display	The car display is the HMI between the driver and the lane assistance item. It displays the status information of the lane assistance item to the driver.
Car Display ECU - Lane Assistance On/Off Status	The lane assistance on/off status part of the display ECU sends the on/off status of the lane assistance item to the car display.
Car Display ECU - Lane Assistant Active/Inactive	The lane assistance active/inactive part receives the information from camera ECU if lane assistance item is active or inactive. Then it sends it to the car display.
Car Display ECU - Lane Assistance malfunction warning	The lane assistance malfunction warning part receives the information if the lane assistance item has some malfunctions from the electronic power steering ECU. Then it sends the information to the car display to enable warning light.
Driver Steering Torque Sensor	The driver steering torque sensor measures the steering torque applied by the driver.
Electronic Power Steering (EPS) ECU - Driver Steering Torque	The EPS ECU Driver Steering Torque part calculates the steering torque which should be applied to the steering wheel based on the steering torque applied by the driver.
EPS ECU - Normal Lane Assistance Functionality	The EPS ECU Normal Lane Assistance Functionality part receives the steering torque request from Camera ECU for LDW and LKA functions. Based the request it calculates the steering torque which should be applied to the steering wheel.
EPS ECU - Lane Departure Warning Safety Functionality	The lane departure warning safety functionality detects malfunctions of the system when the safety goals of lane departure warning function are

	violated.
EPS ECU - Lane Keeping Assistant Safety Functionality	The lane keeping safety functionality detects malfunctions of the system when the safety goals of lane assistance function are violated.
EPS ECU - Final Torque	The EPS ECU final torque combines the steering torque from the driver steering torque and the lane assistance functionality and drives the steering motor.
Motor	The motor is controlled by the EPS ECU and it applies the final steering torque to 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	EPS ECU - LDW Safety Functionality	The LDW functionality shall be turned off and the 'LDW_Torque_Request' shall be 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	50 ms	EPS ECU – LDW Safety Functionality	The LDW functionality shall be turned off and the 'LDW_Torque_Request' 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	EPS ECU - LDW Safety Functionality	The LDW functionality shall be turned off and the 'LDW_Torque_Request' shall be 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 and Integrity Check	The LDW functionality shall be turned off and the 'LDW_Torque_Request' 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	EPS ECU – Safety Startup	The LDW functionality shall be turned off and the 'LDW_Torque_Request' shall be set to zero.

[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 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 Functionality	The LDW functionality shall be turned off and the 'LDW_Torque_Request' shall be 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	50 ms	EPS ECU - LDW Safety Functionality	The LDW functionality shall be turned off and the 'LDW_Torque_Request' 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	EPS ECU - LDW Safety Functionality	The LDW functionality shall be turned off and the 'LDW_Torque_Request' shall be 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 and Integrity Check	The LDW functionality shall be turned off and the 'LDW_Torque_Request' 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	EPS ECU – Safety Startup	The LDW functionality shall be turned off and the 'LDW_Torque_Request' shall be set to zero.

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 LDW safety component shall ensure that the amplitude of the 'LKA_Torque_Request' sent to the 'Final electronic power steering Torque' is applied only for “Max_Duration”.	B	500 ms	EPS ECU - LKA Safety Functionality	The LKA functionality shall be turned off and the 'LKA_Torque_Request' shall be set 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.	B	500 ms	EPS ECU - LKA Safety Functionality	The LKA functionality shall be turned off and the 'LKA_Torque_Request' shall be set to zero.
Technical Safety Requirement 03	As soon as a failure is detected by the LKA safety function, it shall deactivate the LKA feature and the 'LKA_Torque_Request' shall be set to zero.	B	500 ms	EPS ECU – LKA Safety Functionality	The LKA functionality shall be turned off and the 'LKA_Torque_Request' shall be set

					to zero.
Technical Safety Requirement 04	The validity and integrity of the data transmission for 'LKA_Torque_Request' signal shall be ensured.	B	500 ms	EPS ECU - Data Transmission and Integrity Check	The LKA functionality shall be turned off and the 'LKA_Torque_Request' 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	EPS ECU – Safety Startup	The LKA functionality shall be turned off and the 'LKA_Torque_Request' shall be set to zero.

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.]

The Figure 2 below shows the refined architecture of the Lane Assistance item. Compared to the functional safety concept two new software components are added to the Power Steering ECU the “Safety Startup” and “Data Transmission and Integrity Check”. These new software components handle the technical safety requirements relating to data transmission integrity and memory tests.

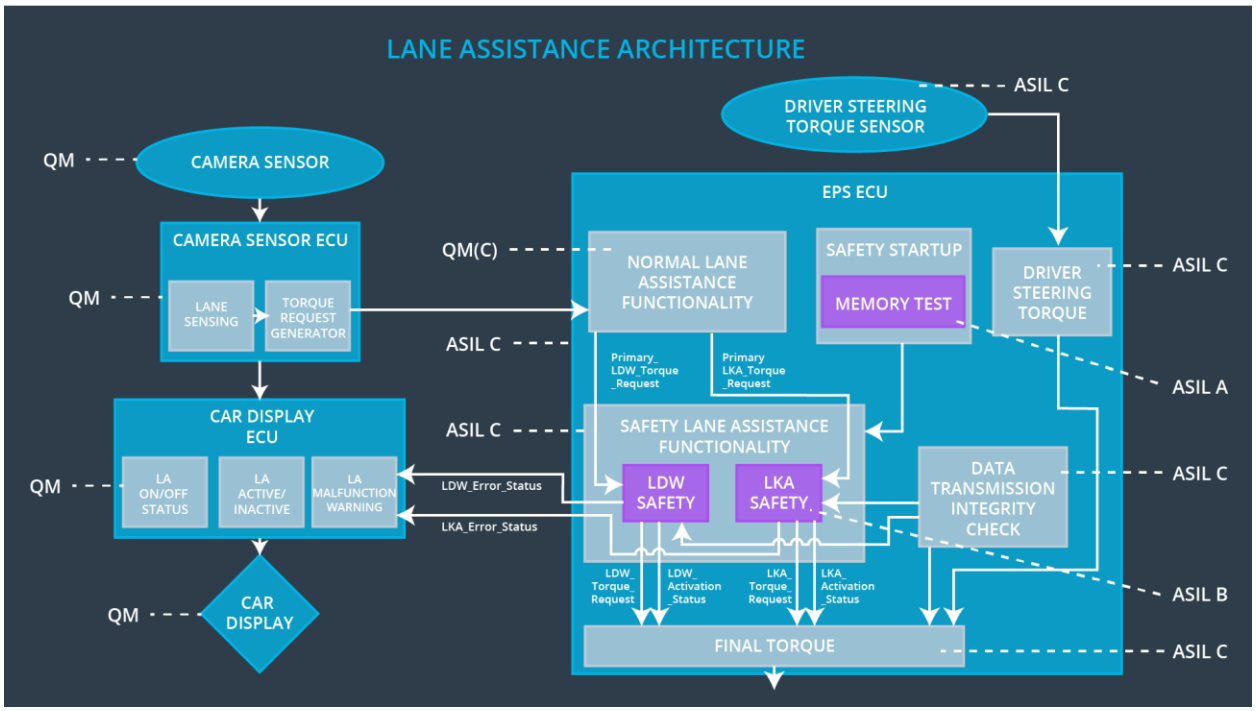

Figure 2: Refined Architecture Technical Safety Concept

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]

The allocation of technical safety requirements are stated in the tables above. It can be seen that all the technical safety requirements are allocated to the Safety LDW and Safety LKA components of the Power Steering ECU except for the requirements relating to data transmission integrity and memory consistency. These technical safety requirements are allocated to the Data Transmission Integrity check and Safety Startup components.

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	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	LDW function turned off	The amplitude or frequency of the oscillating steering torque is greater than Max_Torque_Amplitude or Max_Torque_Frequency.	Yes	Warning lamp turned on
WDC-02	LKA function turned off	The steering torque is provided longer than Max_Duration.	Yes	Warning lamp turned on