Elektrobit

UDACITY

Technical Safety Concept Lane Assistance

Document Version: 1.0

Document history

Date	Version	Editor	Description
11.03.2018	1.0	Nathan Greco	First Draft

Table of Contents

Purpose of the Technical Safety Concept

The technical safety concept is a component level plan that defines both the architecture being implemented and the safety goals necessary to ensure the system satisfies ISO 26262.

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	Apply limits to frequency and magnitude of haptic feedback to steering wheel to prevent interference with driver control	D	100 ms	LDW Disabled with visual indication
Functional Safety Requirement 01-02	Provide a visual indication when the system is enabled but not able to detect the road lanes and correct vehicle position	QM	500 ms	LDW Disabled with visual indication
Functional Safety Requirement 02-01	Create a response window that if a torque command is not executed within a set time the system disables	C	100 ms	LKA Disabled with visual indication
Functional Safety Requirement 02-02	Provide a visual indication when the system is enabled but not able to detect the road lanes and correct vehicle position	QM	500 ms	LKA Disabled with visual indication

Refined System Architecture from Functional Safety Concept

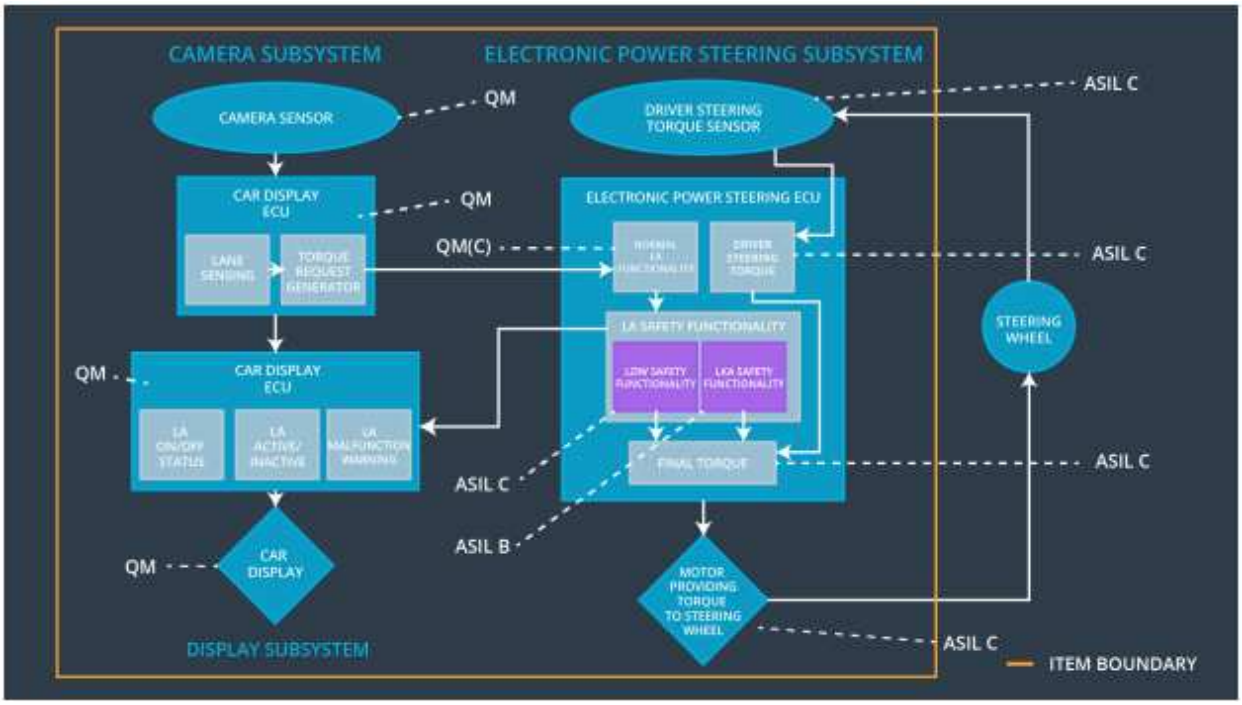

Figure 1 – Detailed system architecture with ASIL ratings

Functional overview of architecture elements

Element	Description
Camera Sensor	Camera device that retrieves images of the road in front of the vehicle
Camera Sensor ECU - Lane Sensing	Process within ECU which processes image from the camera sensor with computer vision algorithms to determine the vehicles relative position to the lane, used by both LDW and LKA systems
Camera Sensor ECU - Torque request generator	Process within ECU which generates the torque to be commands for the motor
Car Display	An informative display to display the road lines and their orientation, display warning and alert messages, and is the primary GUI for the vehicle operator
Car Display ECU - Lane Assistance On/Off Status	Process within the ECU which determines the lane assist system's on/off status
Car Display ECU - Lane Assistant	Process within the ECU which determines the lane

Active/Inactive	assist system's active statys
Car Display ECU - Lane Assistance malfunction warning	Process within the ECU which monitors the health of the LKA system and alerts the driver to faults in the system
Driver Steering Torque Sensor	A sensor that measures that amount of effort the driver is making to steer the vehicle. This is important so that we do not interfere with intentional steering commands from the driver and impede his ability to control the vehicle
Electronic Power Steering (EPS) ECU - Driver Steering Torque	Process with handles torque requests and drives the command of the motor
EPS ECU - Normal Lane Assistance Functionality	Process within the EPS ECU that manages the overall modes and state machine of the system
EPS ECU - Lane Departure Warning Safety Functionality	Process within the EPS ECU that checks the health of the LDW system and triggers any necessary safety modes
EPS ECU - Lane Keeping Assistant Safety Functionality	Process within the EPS ECU that checks the health of the LKA system and triggers any necessary safety modes
EPS ECU - Final Torque	Process within the EPS ECU that generates the final torque command
Motor	The actuator that directly influences the steering of the vehicle. It receives its command from the power steering ECU

Technical Safety Concept

Technical Safety Requirements

Lane Departure Warning (LDW) Requirements:

Functional Safety Requirement 01-01 with its associated system elements

ID	Functional Safety Requirement	Electronic Power	Camera ECU	Car Display ECU

		Steering ECU		
Functional Safety Requirement 01-01	Apply limits to frequency and magnitude of haptic feedback to steering wheel to prevent interference with driver control	**X**		**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 must check the magnitude of the torque command against a min/max threshold	D	100 ms	LDW System	LDW Disabled with visual indication
Technical Safety Requirement 02	The LDW safety component must check the frequency of the torque command against a min/max threshold	D	100 ms	LDW System	LDW Disabled with visual indication

Functional Safety Requirement 01-2 with its associated system elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU
Functional Safety Requirement 01-02	Provide a visual indication when the system is enabled but not able to detect the road lanes and correct vehicle position		**X**	**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 03	The LDW safety component must continuously check that valid road lanes have been detection and a vehicle position identified	QM	500 ms	LDW System	LDW Disabled with visual indication

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 01	Perform a study to determine minimum noticeable magnitude torque commands for a driver to notice the alter and maximum for the driver to maintain control of the vehicle	Impose these limits and attempt to create commands outside these limits to verify the actuator does not actuate at these values
Technical Safety Requirement 02	Perform a study to determine minimum noticeable frequency torque commands for a driver to notice the alter and maximum for the driver to maintain control of the vehicle	Impose these limits and attempt to create commands outside these limits to verify the actuator does not actuate at these values
Technical Safety Requirement 03	Evaluate frequency and duration of interruptions to the lane detection status and determine a time delay that would not pickup false positives	Operate the vehicle and blind the camera so road lanes are not detected. Verify that the vehicle alerts the driver within the identified time window

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	Evaluate typical controller response time and tuning to determine what an acceptable	**X**		**X**

	response time is.			

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 04	The LKA safety component must continuously check that the actual torque command is does not exceed a delay from the command	C	100	LKA System	LKA Disabled with visual indication

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 02-02	Perform study for best means of indication to a driver that the LDW system fails to detect road lane		**X**	**X**

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

ID	Technical Safety Requirement	ASIL	Fault Tolerant Time Interval	Allocation to Architecture	Safe State
Technical Safety Requirement 05	The LKA safety component must continuously check that valid road lanes have been detection and a vehicle position identified	QM	500 ms	LDW System	LDW Disabled with visual indication

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Technical Safety Requirement 04	Evaluate the typical response time of the actuator to determine what would be abnormal operations	Disable the motor and send a command to verify the system detects the delayed response within the time window
Technical Safety Requirement 05	Evaluate frequency and duration of interruptions to the lane detection status and determine a time delay that would not pickup false positives	Operate the vehicle and blind the camera so road lanes are not detected. Verify that the vehicle alerts the driver within the identified time window

Refinement of the System Architecture

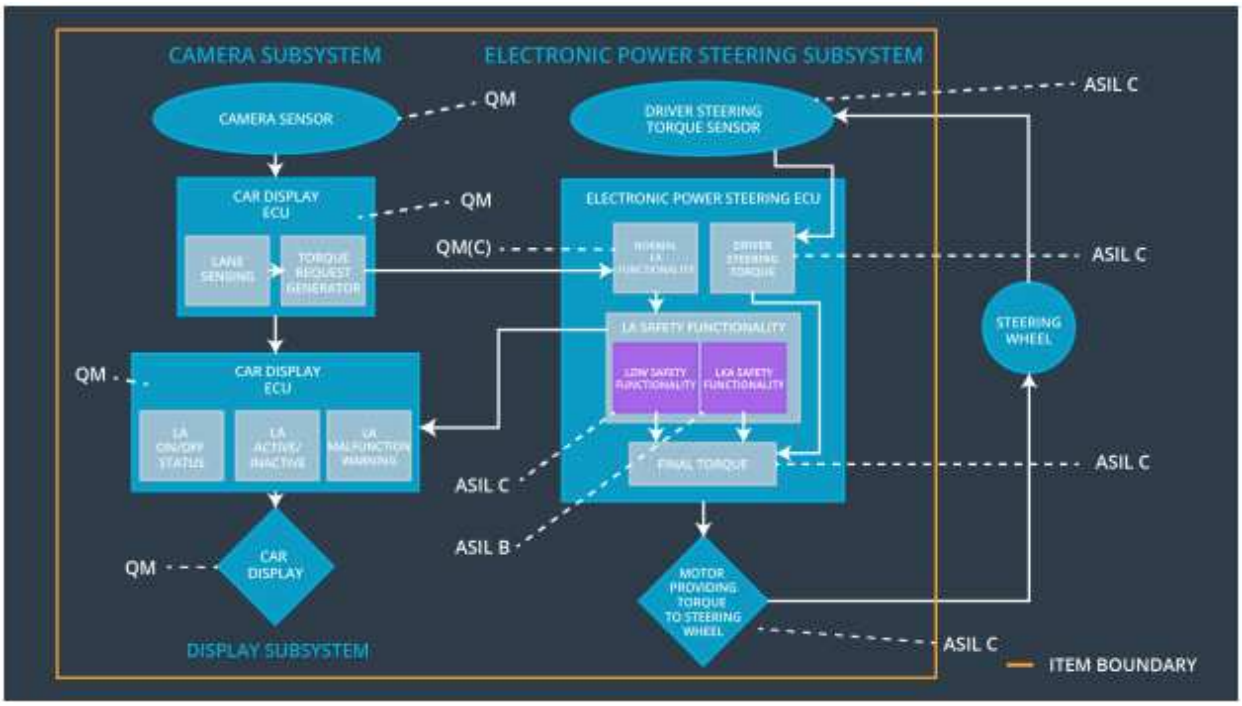

Figure 2 – Detailed system architecture with ASIL ratings

Allocation of Technical Safety Requirements to Architecture Elements

ID	Functional Safety Requirement	Electronic Power Steering ECU	Camera ECU	Car Display ECU

Functional Safety Requirement 01-01	Apply limits to frequency and magnitude of haptic feedback to steering wheel to prevent interference with driver control	**X**		**X**
Functional Safety Requirement 01-02	Provide a visual indication when the system is enabled but not able to detect the road lanes and correct vehicle position		**X**	**X**
Functional Safety Requirement 02-01	Evaluate typical controller response time and tuning to determine what an acceptable response time is.	**X**		**X**
Functional Safety Requirement 02-02	Perform study for best means of indication to a driver that the LDW system fails to detect road lane		**X**	**X**

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01	Disable LDW and alert	Malfunction_01	Yes	Driver indication of fault in LDW system
WDC-02	Disable LDW and alert	Malfunction_02	Yes	Driver indication of fault in LDW system
WDC-03	Disable LKA and alert	Malfunction_03	Yes	Driver indication of fault in LKA system
WDC-04	Disable LDW and alert	Malfunctin_04	Yes	Driver indication of fault in LDW system
WDC-05	Disable LKA and alert	Malfunction_05	Yes	Driver indication of fault in LKA

				system