Elektrobit

UDACITY

Functional Safety Concept Lane Assistance

Document Version: 1.1, Submitted on 2018-09-02
Template Version: 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
8/27/2018	1.0	Nathan	First Creation
9/2/2018	1.1	Nathan	Error Corrected

Table of Contents

Purpose of the Functional Safety Concept

The main purpose of the functional safety concept is to identify requirements and allocate these requirements to system diagrams. Each of these requirements has following specified attributes:

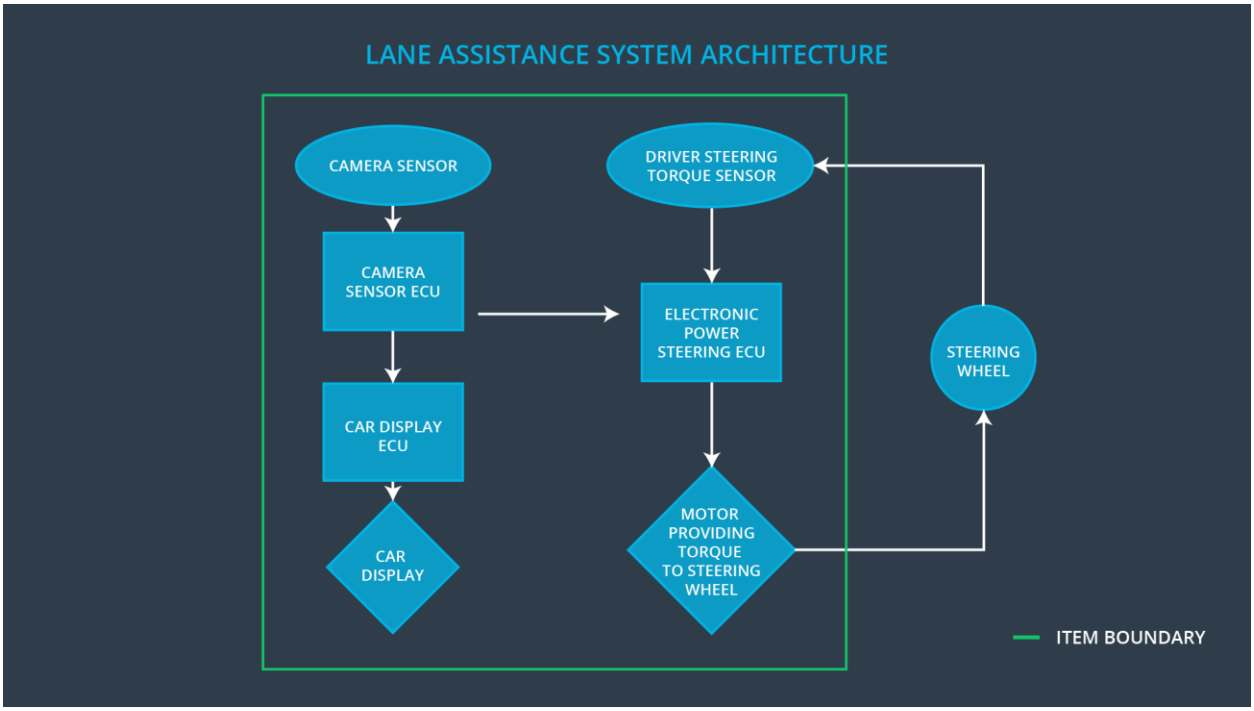
1. ASIL level
2. Fault tolerance time interval
3. Safe state

Inputs to the Functional Safety Concept

Safety goals from the Hazard Analysis and Risk Assessment

ID	Safety Goal
Safety_Goal_01	The oscillating steering torque from the lane departure warning function shall be limited
Safety_Goal_02	The lane keeping assistance function shall be time limited, and the additional steering torque shall end after a given time interval so that the driver cannot misuse the system for autonomous driving
Safety_Goal_03	The camera sensitivity to the luminous intensity shall be above of the minimum required specification (or response sensitivity shall be quicker than a given time interval)
Safety_Goal_04	The lane keeping assistance function shall be stopped and warn the driver in case when electronic power steering ECU exhibit an erratic behavior from overheating.

Preliminary Architecture



Description of architecture elements

Element	Description
Camera Sensor	Continuously reads in images from the road
Camera Sensor ECU	Identifies road lane from the images taken by camera sensor and sends messages to other ECU's when the vehicle deviates from the lane
Car Display	Shows warning on the screen when deviation from lane is detected
Car Display ECU	Controls car display when receiving deviation messages from camera sensor ECU
Driver Steering Torque Sensor	Measures torque applied to the steering wheel
Electronic Power Steering ECU	Calculate in which direction and what amount the steering torque should be applied in order to stay in the lane
Motor	Apply torque to the steering base on the value calculated by electronic power steering ECU

Functional Safety Concept

The functional safety concept consists of:

- Functional safety analysis
- Functional safety requirements
- Functional safety architecture
- Warning and degradation concept

Functional Safety Analysis

Malfunction ID	Main Function of the Item Related to Safety Goal Violations	Guidewords (NO, WRONG, EARLY, LATE, MORE, LESS)	Resulting Malfunction
Malfunction _01_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	The LDW is giving MORE torque amplitude than what is safe	The LDW function applies an oscillating torque with very high torque amplitude (above limit)
Malfunction _01_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback	The LDW is giving MORE torque frequency than what is safe	The LDW function applies an oscillating torque with very high torque frequency (above limit)
Malfunction _02_01	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	The LKA function has NO time limit duration	The LKA function is not limited in time duration which leads to misuse as an autonomous driving function
Malfunction _03_01	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback & Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	The camera sensor used for the LDW and LKA is LESS light sensitivity (low lux change) than what is safe	THE LDW and LKA functions are inoperative at sudden change of luminous intensity with very low lux change
Malfunction _03_02	Lane Departure Warning (LDW) function shall apply an oscillating steering torque to provide the driver a haptic feedback & Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	The camera sensor used for the LDW and LKA is LATE on light sensitivity change than what is safe	THE LDW and LKA functions are inoperative at sudden change of luminous intensity with very high change frequency
Malfunction _04_01	Lane Keeping Assistance (LKA) function shall apply the steering torque when active in order to stay in ego lane	The electronic power steering ECU has bad heat dissipation, making it MORE heated than what is safe	The LKA function is delayed due to electronic power steering ECU overheating, unable to apply steering torque on time at a sharp turn

Functional Safety Requirements

Lane Departure Warning (LDW) 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	D	50 ms	The lane departure oscillating torque amplitude is below Max_Torque_Amplitude
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	D	50 ms	The lane departure oscillating torque frequency is below Max_Torque_Frequency
Functional Safety Requirement 03-01	The lane keeping item shall ensure that the light sensitivity change of lane departure camera ECU is higher than Min_Lumen_Change	B	20 ms	The light sensitivity change of lane departure camera sensor is higher than Min_Lumen_Change
Functional Safety Requirement 03-02	The lane keeping item shall ensure that the light sensitivity change of lane departure camera sensor is below than Max_Lumen_Frequency	B	20 ms	The light sensitivity change of lane departure camera sensor is below than Max_Lumen_Frequency

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 01-01	Make sure that the lane departure oscillating torque amplitude is below Max_Torque_Amplitude, test how drivers react to different torque amplitude to prove the value is appropriate	The lane assistance output is set to zero within the 50 ms fault tolerant time interval, do software test inserting different amplitude values
Functional Safety Requirement 01-02	Make sure that the lane departure oscillating torque frequency is below Max_Torque_Frequency, test how drivers react to different torque frequency to prove the value is appropriate	The lane assistance output is set to zero within the 50 ms fault tolerant time interval, do software test inserting a fault value in different time intervals

Functional Safety Requirement 03-01	Make sure that the lane departure camera sensor light sensitivity is higher than Min_Lumen_Change, test how lane assistance item responds to different lux to prove the value is appropriate	The lane assistance camera captures clear video image within the 20 ms fault tolerant time interval, do software test inserting different lumen values
Functional Safety Requirement 03-02	Make sure that the lane departure camera sensor light sensitivity frequency is lower than Max_Lumen_Frequency, test how lane assistance item responds to different frequency to prove the value is appropriate	The lane assistance camera captures clear video image within the 20 ms fault tolerant time interval, do software test inserting a fault value in different time intervals

Lane Keeping Assistance (LKA) Requirements:

ID	Functional Safety Requirement	ASIL	Fault Tolerant Time Interval	Safe State
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only up to Max_Duration	B	500 ms	The lane keeping assistance torque apply duration is below Max_Duration
Functional Safety Requirement 04-01	The electronic power steering ECU shall monitor its heat temperature and disables LKA when exceeding Max_Temp	QM	100 ms	The lane keeping assistance electronic power steering ECU heat temperature is below Max_Temp
Functional Safety Requirement 04-02	The car display ECU shall notify LKA function is disabled, Car_Display is on when Max_Temp is exceeded	QM	20 ms	The lane keeping assistance Car_Display is on when Max_Temp is exceeded

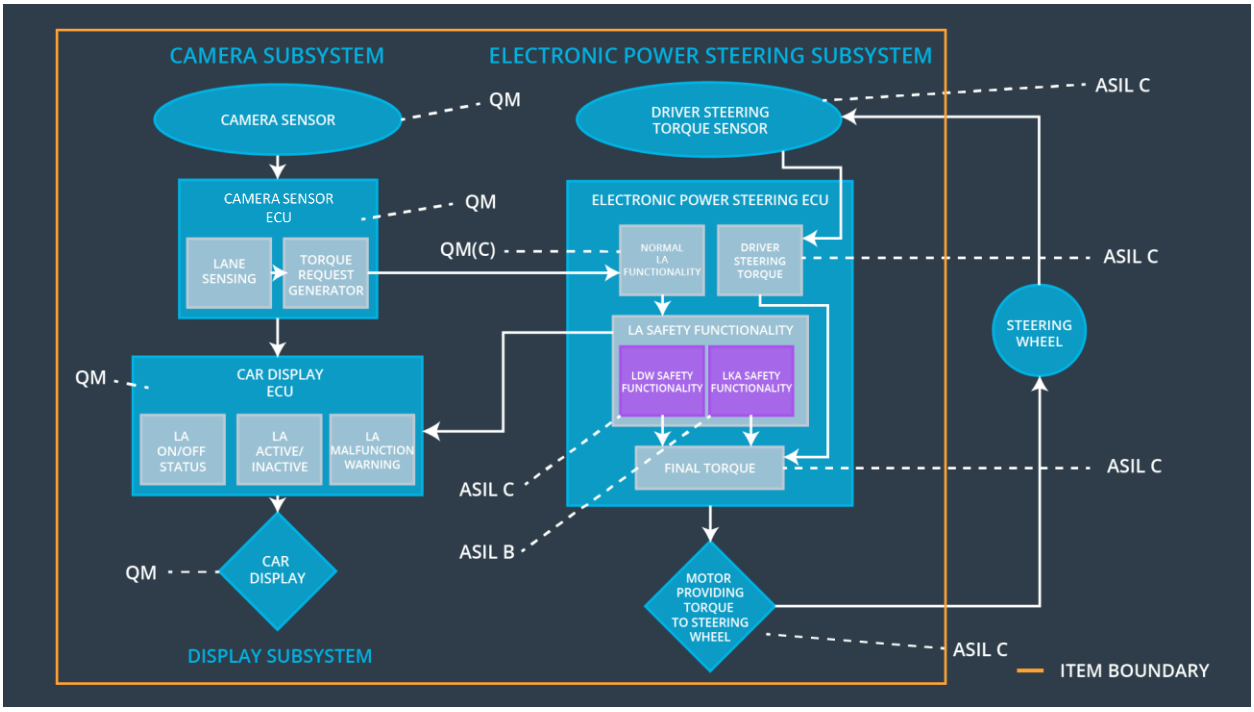
* Functional safety requirements for Malfunction_03_01 and Malfunction_03_02 are omitted due to be duplicated in LDW requirements.

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

ID	Validation Acceptance Criteria and Method	Verification Acceptance Criteria and Method
Functional Safety Requirement 02-01	Make sure that the torque applied duration from electronic power steering ECU is lower than Max_Duration, test how drivers react to different torque duration to prove the value is appropriate	The lane assistance output is set to zero within the 500 ms fault tolerant time interval, do software test inserting different duration values

Functional Safety Requirement 04-01	Make sure that the lane assistance is disabled when heat temperature reading of power steering ECU is higher than Max_Temp, test how much drivers react quick enough to the LKA function gets disabled to prove the value is appropriate	The lane assistance output is set to zero within the 100 ms fault tolerant time interval, do software test inserting different duration values
Functional Safety Requirement 04-02	Make sure that the Car_Display notification is on when heat temperature reading of power steering ECU is higher than Max_Temp, test how much drivers react quick enough to the LKA function gets disabled to prove the value is appropriate	The lane assistance output is on within the 20 ms fault tolerant time interval, do software test inserting different duration values

Refinement of the System Architecture



Allocation of Functional Safety Requirements to Architecture Elements

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		
Functional Safety Requirement 01-02	The lane keeping item shall ensure that the lane departure oscillating torque frequency is below Max_Torque_Frequency	X		
Functional Safety Requirement 02-01	The electronic power steering ECU shall ensure that the lane keeping assistance torque is applied for only up to Max_Duration	X		
Functional Safety Requirement 03-01	The lane keeping item shall ensure that the light sensitivity change of lane departure camera sensor is higher than Min_Lumen_Change		X	
Functional Safety Requirement 03-02	The lane keeping item shall ensure that the light sensitivity change of lane departure camera sensor is below than Max_Lumen_Frequency		X	
Functional Safety Requirement 04-01	The electronic power steering ECU shall monitor its heat temperature and disables LKA when exceeding Max_Temp	X		

Warning and Degradation Concept

ID	Degradation Mode	Trigger for Degradation Mode	Safe State invoked?	Driver Warning
WDC-01_01	Turn off	Oscillating torque amplitude is higher than Max_Torque_Amplitude	Yes	Warning light on the dashboard
WDC-01_02	Turn off	Oscillating torque frequency is higher than Max_Torque_Frequency	Yes	Warning light on the dashboard
WDC-02_01	Turn off	The lane keeping assistance stays on for longer than Max_Duration	Yes	Warning light on the dashboard
WDC-03_01	Turn off	The light sensitivity change exceeds a threshold Min_Lumen_Change	Yes	Warning light on the dashboard
WDC-03_02	Turn off	The light sensitivity change exceeds a threshold Max_Lumen_Frequency	Yes	Warning light on the dashboard
WDC-04_01	Turn off	The lane keeping assistance electronic power steering ECU heat temperature is higher than Max_Temp	Yes	Warning light on the dashboard