Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
3/13/2018	1.0	David Simon	First attempt
3/21/2018	2.0	David Simon	Refine purpose, development interface agreement, remove instructions
3/23/2018	3.0	David Simon	Content source – Udacity lectures, refine item definition and confirmation measures
3/24/2018	4.0	David Simon	Change bimonthly auditing role to safety auditor

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan provides an overall description of the lane assistance item consisting of the lane departure warning and lane keeping assistance systems, the goals and safety measures, the roles and responsibilities of the tier-1 organization and the original equipment manufacturer (OEM) in the development interface agreement, and the confirmation measures needed for the functional safety of the lane assistance item.

Scope of the Project

For the lane assistance project, the following safety lifecycle phases are in scope:

- Concept phase
- Product Development at the System Level
- Product Development at the Software Level

The following phases are out of scope:

- Product Development at the Hardware Level
- Production and Operation

Deliverables of the Project

The deliverables of the project are:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept
- Software Safety Requirements and Architecture

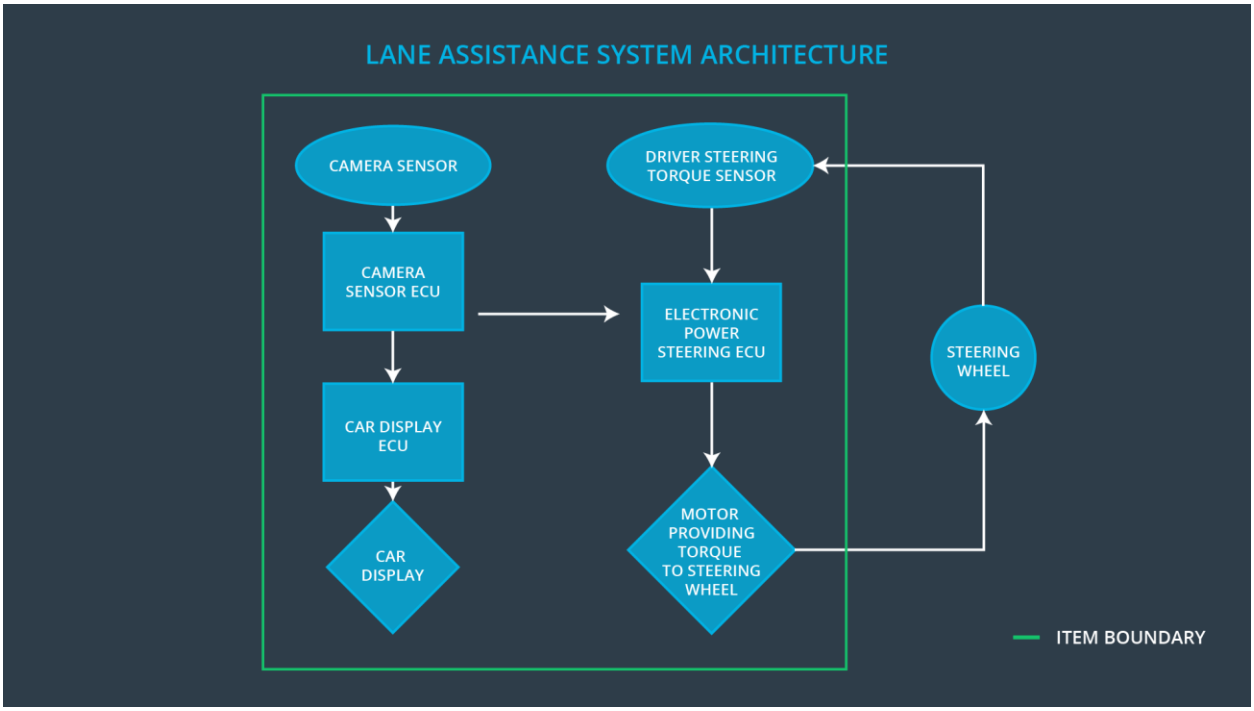
Item Definition

The item is the lane assistance system for lane departure warning and lane keeping assistance which improves safety by monitoring the car's location relative to the lane line boundaries.

The lane departure warning (LDW) alerts the driver of impending unintended lane line crossing. The lane keeping assistance (LKA) helps to maintain the vehicle within the lane. LDW vibrates the steering wheel to alert the driver of the lane crossing. LKA moves the steering wheel back toward the lane center to maintain the car within the lane.

The camera subsystem detects the car location relative to the lane lines. This subsystem consists of the camera sensor and the camera electronic control unit (ECU). The power steering subsystem applies the vibration and movement for the LDW and LKA functions. This subsystem consists of the driver steering torque sensor, the electronic power steering ECU, and the motor providing torque to the steering wheel. The car display subsystem notifies the driver of the LDW and LKA operation. This subsystem consists of the car display ECU and the car display.

The lane assistance boundary includes the camera, power steering, and car display subsystems. The steering wheel is outside the item boundary. This is depicted in the following diagram.



OPTIONAL

Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

- **Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc**
- **Legal requirements in your country for lane assistance technology**
- **National and International Standards Related to the Item**
- **Records of previously known safety-related incidents or behavioral shortfalls**

Goals and Measures

Goals

The goal of this project is to analyze the lane assistance functions with ISO 26262 to minimize the hazards and potential injury associated with any malfunction of the lane assistance system consisting of the lane departure warning and the lane keeping assistance functions.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	All Team Members	Constantly
Coordinate and document the planned safety activities	Project Manager	Constantly
Allocate resources with adequate functional safety competency	Project Manager	Within 2 weeks of start of project
Tailor the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Plan the safety activities of the safety lifecycle	Safety Manager	Within 4 weeks of start of project
Perform regular functional safety audits	Safety Auditor	Once every 2 months
Perform functional safety pre-assessment prior to audit by external functional safety assessor	Safety Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

Safety is the highest priority of the company, even above the importance of deadlines and costs. Working groups will operate independently from auditors with design decisions dated, documented and thereby traceable to individuals within the group. Safety will be rewarded, and shortcuts will be penalized. Communication of any safety problem will be encouraged.

Safety Lifecycle Tailoring

For the lane assistance project, the following safety lifecycle phases are in scope:

Concept phase
Product Development at the System Level
Product Development at the Software Level

The following phases are out of scope:

Product Development at the Hardware Level
Production and Operation

Roles

Role	Org
Functional Safety Manager- Item Level	OEM
Functional Safety Engineer- Item Level	OEM
Project Manager - Item Level	OEM
Functional Safety Manager- Component Level	Tier-1
Functional Safety Engineer- Component Level	Tier-1
Functional Safety Auditor	OEM or external
Functional Safety Assessor	OEM or external

Development Interface Agreement

1. The purpose of a development interface agreement is to detail the roles and responsibilities of the tier-1 organization and the original equipment manufacturer (OEM) in the development of lane keeping assistance system. Evidence and work products required of the tier-1 organization and the OEM supplier of the lane assistance system are also clearly specified in the development interface agreement. Compliance will follow the safety guidelines of ISO 26262. The development interface agreement helps avoid disputes between the tier-1 organization and the original equipment manufacturer.

2. Under direction of the Project Manager, the OEM will develop and test the lane keeping assistance module following the required specifications of the tier-1 organization. Under direction of the functional safety manager, David Simon, the tier-1 organization will prioritize safety in determining the required specifications. The functional safety manager at the OEM will oversee the functional safety engineer and the development team at the OEM. The functional safety engineer, David Simon, of the tier-1 organization and the functional safety engineer of the OEM will work together to resolve any issues that arise during the development process. The external functional safety auditor will bimonthly audit the developing lane assistance system for proper functioning according to the safety goals. Upon delivery of the completed lane keeping assistance module, the external functional safety assessor will fully test the integrated lane keeping system for proper functioning. The functional safety engineer, David Simon, of the tier-1 organization and the functional safety engineer of the OEM will work together to resolve any issues that arise during the system tests, completing modifications necessary to comply with the requisite safety specifications for the lane keeping assistance system.

Confirmation Measures

Confirmation measures are needed to assure the vehicle with the applied lane assistance system does make the vehicle safer, and the safety protocol follows the safety plan and the guidelines of ISO 26262.

A confirmation review is done periodically over the course of the design and development period to assess the project compliance with the ISO 26262 standard. This will be conducted by an independent person not directly involved with the work groups. These pre-audits before the functional safety audit are usually conducted by the safety manager.

A functional safety audit is conducted by the independent safety auditor after the product implementation to determine its compliance with the safety plan.

A functional safety assessment is usually conducted by an independent safety assessor to confirm that the implemented system does improve functional safety.

A safety plan could have other sections that we are not including here. For example, a safety plan would probably contain a complete project schedule.

There might also be a "Supporting Process Management" section that would cover "Part 8: Supporting Processes" of the ISO 26262 functional safety standard. This would include descriptions of how the company handles requirements management, change management, configuration management, documentation management, and software tool usage and confidence.

Similarly, a confirmation measures section would go into more detail about how each confirmation will be carried out.