Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
20/10/2018	1.0	L.R	First submission

Table of Contents

Introduction

Purpose of the Safety Plan

Vehicles are complex systems that require a comprehensive approach to safety. This plan defines roles and responsibilities and outlines the steps taken to achieve functional safety. Documentation includes:

- Safety Culture
- Safety Lifecycle
- Safety Management Roles and Responsibilities
- Development Interface Agreements
- Confirmation Measures

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 Lane Assistance System (LAS) alerts drivers of accidental lane changes and attempts to correct steering to remain in the current lane. There are two main functions of this system:

- lane departure warning (LDW)
- lane keeping assistance (LKA)

If the vehicle starts changing lanes without using a turn signal, the LAS will assume that the driver has become distracted and leaving the lane was not intended. The system will vibrate the steering wheel (lane departure warning) and also move the steering wheel back towards the lane center (lane keeping assistance).

When LDW is active, the system shall apply an oscillating steering torque to provide the driver a haptic feedback. When LKA is active, the system shall apply the steering torque in order to stay in ego lane. These functions are activated by lane drift detection. Lane drift detection comes from the camera sub-system. Lane drift detection also activates a warning light in the car display sub-system to indicate to the driver LAS activation. The LAS is deactivated by using the turn signal or by manually turning it off with a button.

The LAS expects the driver to have both hands on the steering wheel at all times. LKA only applies the necessary extra torque to center the vehicle, which is calculated by sensing the torque already being applied by the driver.

The LAS includes the Camera sub-system, Electronic Power Steering sub-system, and the Car Display sub-system. The components of these sub-systems are identified in Figure 1.

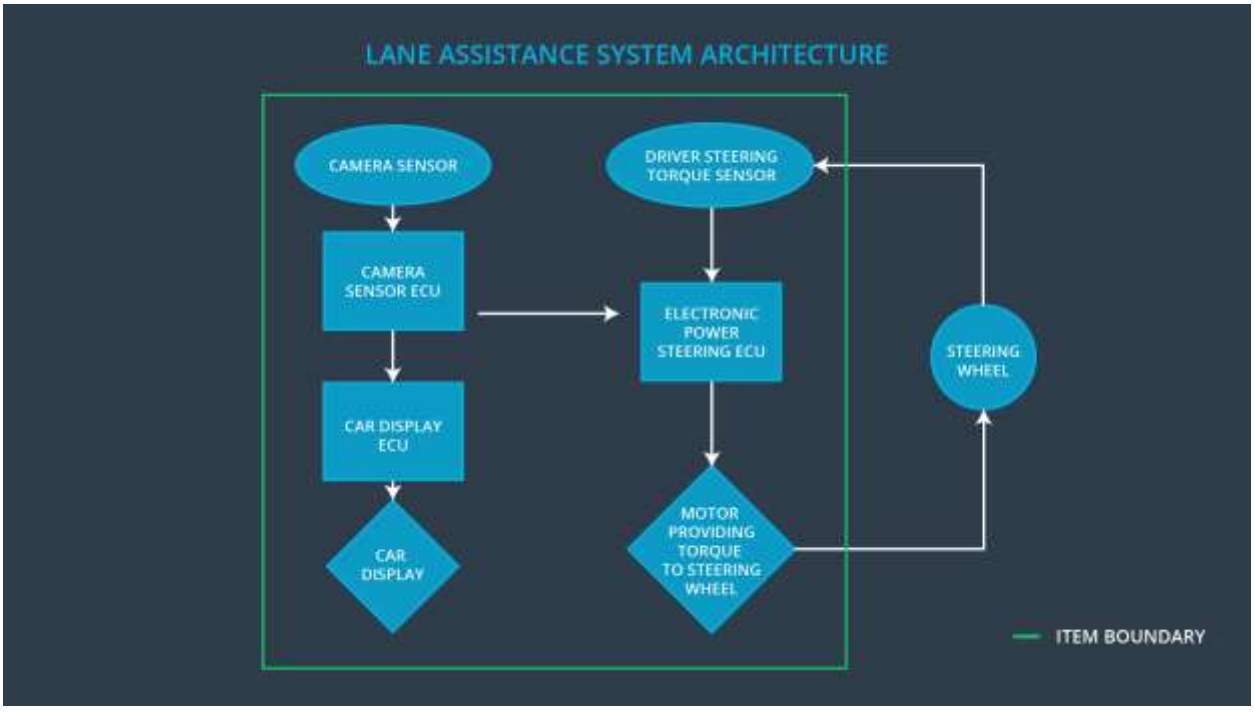

Figure 1 - Lane Assistance System Architecture

Goals and Measures

Goals

The project goals are:

- Identify hazards and high risk situations which may result from a failure of the Lane Assistance System
- Measure the risk
- Lower the risk through systems engineering techniques to acceptable levels.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All	Constantly
Create and sustain a safety culture	All	Constantly
Coordinate and document the planned safety activities	Safety 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 Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

Organizational procedures and culture play a large role in the safety outcomes of products developed by that organization. A safety culture that implements clear policies about what to do

in case of design problems supports the development, production and operation of safe systems. The following characteristics have been identified as key to a successful safety culture:

- High priority: safety has the highest priority among competing constraints like cost and productivity
- Accountability: processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- Rewards: the organization motivates and supports the achievement of functional safety
- Penalties: the organization penalizes shortcuts that jeopardize safety or quality
- Independence: teams who design and develop a product should be independent from the teams who audit the work
- Well defined processes: company design and management processes should be clearly defined
- Resources: projects have necessary resources including people with appropriate skills
- Diversity: intellectual diversity is sought after, valued and integrated into processes
- Communication: communication channels encourage disclosure of problems
- Quality Management: consistently provide products and services that meet requirements

Safety Lifecycle Tailoring

This project modifies a product that already exists, and therefore does not impact all of the steps in the safety lifecycle. New functionality only impacts certain parts of the concept and development phases.
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

Project Manager

- Overall project management
- Acquires and allocates resources needed for the functional safety activities
- Appoints safety manager or might act as safety manager

Safety Manager

- Planning, coordinating and documenting of the development phase of the safety lifecycle
- Tailors the safety lifecycle
- Maintains the safety plan
- Monitors progress against the safety plan
- Performs pre-audits before the safety auditor

Safety Engineer

- Product development
- Integration
- Testing at the hardware, software and system levels

Safety Auditor

- Ensures that the design and production implementation conform to the safety plan and ISO 26262.
- Must be independent from the team developing the project

Safety Assessor

- Independent judgement as to whether functional safety is being achieved via a functional safety assessment
- Must be independent from the team developing the project

Test Manager

- Plans testing activities
- Coordinates testing to show that the vehicle system works correctly

Development Interface Agreement

The purpose of the DIA is to the clearly delineate the boundaries of responsibility between the Tier-1 supplier and OEM. These responsibilities include aspects of design, testing and verification, and production. This helps avoid disputes during the planning and development of the product, and clarifies liability in case of a failure.

For the Lane Assistance System (LAS), if something has gone wrong at the item level, where components are integrated into the final product, the OEM is responsible. However, if the failure is limited to a specific component, then responsibility lies with the Tier-1 supplier. The OEM is

responsible for overall vehicle safety and how the subsystems provided by the Tier-1 integrate with the rest of the vehicle systems. If an individual component, such as lane detection software running on the LAS, has a failure, this is the responsibility of the Tier-1. Tier-1 shall verify functional safety of the supplied sub-systems, and the OEM shall verify functional safety of the integration with other systems.

All involved parties need to agree on the contents of the DIA before the project begins.
The DIA also specifies what evidence and work products each party will provide to prove that work was done according to the agreement. The ultimate goal is to ensure that all parties are developing safe vehicles in compliance with ISO 26262. Both companies agree to the above tailoring of the safety lifecycle. Safety concerns will be shared through the Functional Safety Managers of both companies.

Confirmation Measures

Confirmation measures are designed to confirm the following items:

- Processes comply with the functional safety standard (ISO 26262)
- Project execution is following the safety plan
- Design does actually improve safety

Confirmation measures are used by the FS Auditor & Assessor. The people who fulfill these roles are independent of the people who designed and developed the product. The confirmation review, FS audit and FS assessment are completed with reference to the measures.

The confirmation review ensures project compliance with ISO 26262. This is done by the independent auditor. The auditor also completes the functional safety audit, which checks to make sure that the actual implementation of the project conforms to the safety plan. The FS assessment confirms that plans, designs and developed products actually achieve functional safety and is completed by the independent FS assessor.

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.