Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: Version 1.1, Released on 2018-11-21

Document history

Date	Version	Editor	Description
11/6/2018	1.0	Emile Papillon	First draft
11/21/2018	1.1	Emile Papillon	Review and Release

Table of Contents

Introduction

Purpose of the Safety Plan

The ultimate goal of functional safety is to avoid accidents by reducing risk to acceptable levels. This safety plan will be a valuable tool to put in practice the necessary measures. More specifically, the present safety plan serves the purpose of tailoring the safety lifecycle, stating the roles and responisibilities of each of the stakeholders and specifying the interface agreement. Finally, this safety plan also specifies the confirmation measures.

The tailoring of the safety lifecycle is done by defining if the item is a completely new one or if the scope of the project is to modify existing system. In the latter case, only some aspects of the safety lifecycle need to be covered. The tailoring process takes care of selecting these aspects and documenting how the other ones are already taken in consideration by the existing system. A safety lifecycle involves different participants and the safety plan specifies roles and responsibilities. Typically, a project manager, a safety manager, a safety engineer (or more than one), a safety auditor, a safety assessor and a test manager compose the team related to the safety plan. These participants tasks will be scoped in this safety plan.

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 considered is a simplified version of a lane assistance system.
Functional Description:
A camera subsystem made of a camera sensor and a camera sensor ECU process the road image and sends indormation about road departure to the electronic power steering subsystem which in turn applies torque to the steering wheel to either warn the driver that they are departing the intended lane or to help them maintain their position centered in a lane. If the driver has activated a turn signal, the item won't act. If the driver has turned off the lane keeping feature, it will not output any torque to the steering column. This system is an assist feature and must not be confused with an autonomous feature : the driver must at all time intend to keep control of the vehicle.

The two main functions of this item are lane keeping assist (LKA) and lane departure warning (LDW). They are defined as :

- **LDW** : When a lane departure is determined as imminent by the system, the system will provide a haptic warning. The vehicle quickly moves the steering wheel back and forth to create a vibration to serve as this haptic warning.

- **LDW** : The **l**ane keeping assistance functionality will automatically assist the driver; the lane keeping assistance function will apply the steering torque when active in order to stay in ego lane, unless the driver explicitly expresses will to change lane by using the turn signal. Also, the driver may disable it by the press of a button. This feature is intended to be used as maintains control of the vehicle. In that sense it is a driving assistance feature and not an autonomous feature.

The following subsystems constitute the lane assistance item :
System Architecture
The following section describes how the item's functions are allocated to its different subsystems.
Camera subsystem: The following The camera is responsible of detecting lane markings to assess whether the car is departing the lane or not. It is constituted of the following elements:
- Camera sensor: detects lane markings
- Camera sensor ECU (Electronic Control Unit) : processes raw images

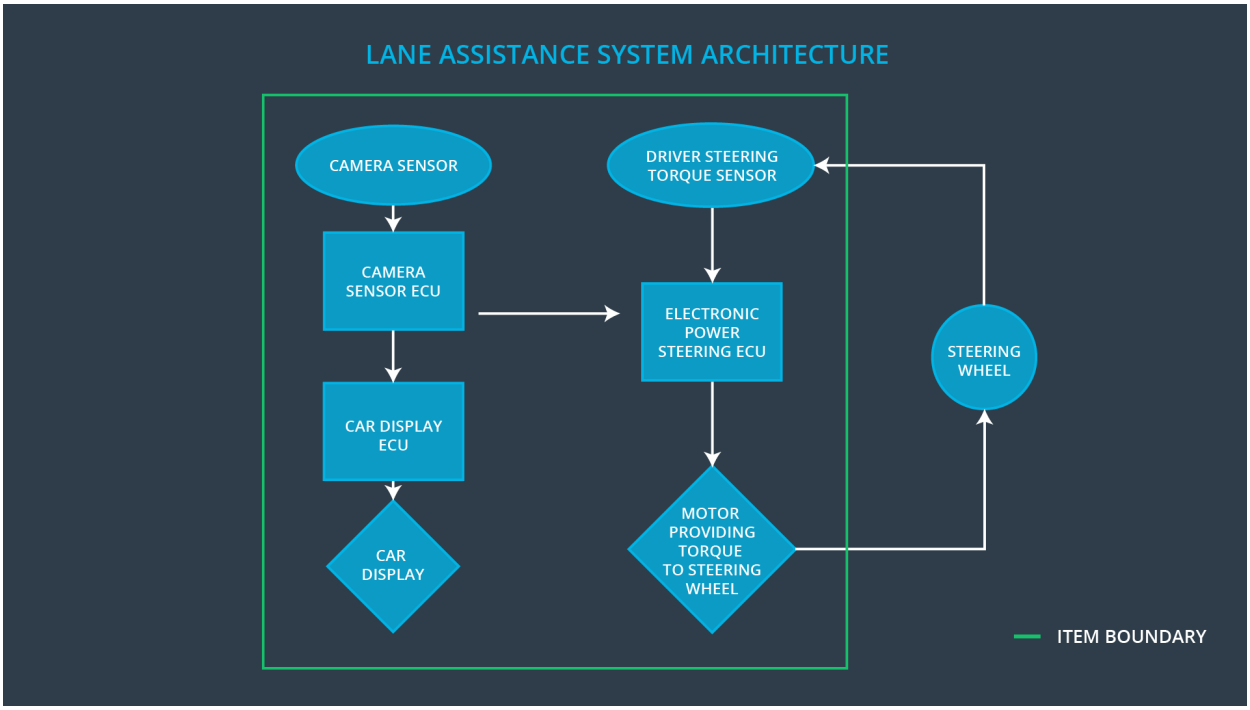
Electronic Power Steering subsystem: The power steering serves as the main actuator of the lane assistance item. It is through this subsystem that the item can assist in steering the vehicle or provide haptic feedback. The power steering is constituted of the following subsystems:
- Driver Steering Torque Sensor : senses the drivers input to control the compensation accordingly.

- Electronic Power Steering ECU: serves as an interface to manage the torque applied.
- Motor Proving Torque to Steering Wheel

Car Display subsystem: The item must be able to display information to the user and it does so through the car display.

- Car Display ECU: interface to the display screen.
- Car Display: displays information to the driver

The following diagram shows the interaction between different subsystems.



Goals and Measures

Goals

The goals of the safety analysis come down to lowering the risks down to acceptable levels. The level of risk is the product of the severity and the probability of a given event. In order to achieve the top level safety goal described above, the hazardous situations are brainstormed and analyzed and are used to derive ASIL levels which in turn are used to derive safety requirements. This process is described by ISO 26262.

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	All Team Members	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

In order to have a safe culture, companies need to prioritize safety over cost or productivity. Employees must be accountable for their decisions. This can be achieved through a good implementation of traceability of decisions up to the decision maker or the group who took the decision. The company also needs to rewards safety and to penalize unsafe attitudes. Any auditing entity shall be independent from the design group or anyone having interest in the success of the endeavor. The process must be well defined and clearly documented and the resources shall be made available to facilitate their implementation. Good communication is also very important to safe practices.

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

The responsibilities of the different stakeholders are defined here with the goal of:

- Avoiding disputes
- Ensuring liability in case of conflict
- Clarifying responsibilities (who is responsible of fixing issues that may arise).

The company will analyze and modify the various sub-systems from a functional safety viewpoint. The OEM will provide a functional Lane Assistance System.

Confirmation Measures

The confirmation measures will ensure that the project is complying with the standards in place (ISO 26262). The confirmation measure's scope also includes insuring that the present safety plan is followed. Furthermore, it will be shown that the project effectively improves the overall safety.

The confirmation review will ensure the compliance of the current project with the standards in place (ISO 26262). It will be performed by an independent, external tier. A functional safety audit will ensure the safety plan is respected. Finally, a functional safety assessment will be performed by another independent auditor that will be responsible of insuring that the project results in an improved safety overall, effectively minimizing risk.

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.