Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
16 May 2018	1.0	Rajagopala Rao Srinadhuni	Overview of the functional safety plan to be followed for Lane Assistance

Table of Contents

Introduction

Purpose of the Safety Plan

The Safety Plan shall provide an overview to the functional safety plan, guiding us on how to plan a safe system. To implement functional safety in a vehicle, we must clearly set what must be accomplished. We shall define roles and outline how to achieve each of them. The vehicle system under analysis shall also be described in this document. Additionally, the document shall talk about the Safety Culture followed, and how the plan actually achieves a safe system.

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

This set of documents shall focus on a Lane Assistance System, which works to monitor a car's position on the road. It checks whether a lane change is intentional and gives a warning and/or control signals to correct changes that are not. The system implemented in our case, follows a sensory warning system, which gives it the name Haptic Lane Feedback System. The following points discuss the main functionalities of the Lane Assist System:

- Lane Departure Warning: Is a warning given when lane change occurs unintentionally, or as defined by the system. Checks are placed on systems such as *turn indictors* or *sensors*, upon whose behavior warnings are issued, in the form of steering vibration (here) or an audible signal
- Lane Keeping Assistance: The vehicle provides assistance, when an unintentional lane change warning is received, to stay in the current lane. This is done by moving the steering gently towards the center of the lane

The following components constitute the Lane Departure Warning functionality:

- Sensors: A variety of sensors may be used to check whether a lane change is unintentional. Cameras are the most widely used sensor, followed by lasers or infra-red or even something as simple as turn indicators

- Warning system: Constitutes a system to warn the driver that an unintentional lane change is being performed. Usually an auditory signal such as a beep or a steering vibration is produced. Our system produces a steering vibration to warn the driver

The Lane Keeping Assistance functionality is comprised of the following sub-system(s):

- Power Steering / Steering Assist: When the Lane Departure System issues a warning, the steering system is activated to produce a reverse torque that slowly corrects the incorrect drift created

Coordinating between the two systems, is a third component, the electronic control unit, described as follows:

- Electronic Control Unit(ECU): Is the brain of the system. Coordinates between sensors and steering assist system, deciding which signal to issue a warning and act upon and which signals to treat as Keep Lane signals

Lastly we shall talk about the system boundaries, where we describe how the Lane Assistance System fits with other functionalities and systems present in the vehicle:

- Camera: The system connects to a camera as sensor to detect when the vehicle moves out of its lane while driving.
- Lane change indicator lamps: When the camera detects a change in lane, it sends a command to the ECU which then check whether the lane change indicators are being used
- ECU: Compares sensor data and issues warning if lane change seems unintentional. Otherwise the system stays latent
- Steering assist: When a lane change warning is issued, the system activates to generate an opposing torque and differ the accidental lane change

The Steering assist and ECU can be seen as components present as part of the Lane Assist System itself. The Camera and lane change indictors work as components outside the system and give their input to the Lane Assist System.

We now have a basic definition of the Item in consideration for this document, to proceed with further definition of the Safety Plan.

Goals and Measures

Goals

ISO 26262 is the standard for establishing functional safety standards. We aim to set a standard for the safety guidelines defined for lane assistance functions, analyzed through ISO 26262 processes. This way we can understand the system we are working with so that

- We understand the working and are able to identify all possible hazards
- Analyze the possible hazards and calculate the risk they produce
- Use this analysis as a basis for introducing checks in our system, when designing the system and implementing the same, so that we take care of vulnerabilities

The ultimate goal is thus to produce a system that is functionally safe, having checks or warnings for hazards that are deemed risky (subject to quantifiers). The ISO standard provides us with a means to establish the same in defined, definite structure.

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 Auditor	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

Safety Culture

Safety of a system is ensured not only by checking the technical aspects but by also maintaining a consistent safety culture at the organizational level. Safety is not a constraint but a necessity in all planning processes. The following points talk about the safety culture followed

- Safety takes highest priority: No other perspective such as cost or profit or a deadline can take precedence over safety. This means that whenever faced with a choice, safety is the only answer
- Safety is a well-defined process: The ISO 26262 standard is followed in maintaining the functional safety of the system, following structured processes and documentation
- Traceability: All steps taken as part of Functional Safety procedure must be well documented, so that each step can be checked against and traced back to its creator. This not only provides a strong, structured base for our purpose but also enforces accountability in the system
- Communication: Ideas are encouraged and everyone is welcome to participate while designing and planning the safety plan
- Independence: The audit team is an independent team, separate from the team designing the safety plan

There must be a constant check to assure that a desired level of excellence in all aspects of safety, which is brought about by using appropriate quality management steps.

Safety Lifecycle Tailoring

The following phases of the safety lifecycle document are within scope of the document:

- Concept Phase: It is important to plan functional safety right from the concept phase. This allows safety to be incorporated in the design itself to ensure a robust system plan that can forsee most (if not all) possible risks
- Product Development at the System Level: By this phase, we have a definite direction to develop our system for. We know how we shall proceed and what the system consists of. Planning for safety becomes more direct and essential, as we now have a system to focus on, with the system structure and functioning in mind
- Product Development at the Software Level: With the system development in place, the software dictates how each the functionality will be achieved and monitored within the

system. Planning for safety for the internal workings shall oversee to it that software malfunctions are accounted for

A few phases shall be kept out of scope of this safety plan as well

- Product Development at the Hardware Level: While we plan how the system functions and where the software works, it is not important on how the hardware is assigned as long as it achieves the desired functionality
- Production and Operation: The functional safety plan accounts for possible risks due to the electrical and electronic components of the system. We plan to make sure to that all functionalities work as they should, the means of accomplishing which lies outside the scope of this document

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 Development Interface Agreement (DIA) delineates roles of the involved stakeholders in a product development plan. The DIA assigns responsibilities for safety and fixes liabilities in case of safety. It defines who the producer is and who shall consume the product, alongwith the requirements and expectations. The product and information to be exchanged between involved parties, with assignment of roles to be carried on with product development are also mentioned here. The interaction between the involved parties, and how resources may be shared, including designs and information are all discussed in this document.

Specifying the nuances of the agreement here allows for clear demarcation of roles and responsibilities, so that no disputes arise in case of failure. It also clarifies who shall be responsible to fix a malfunction in case it occurs. The points below discuss how the various entities involved in the production of the vehicle shall contribute:

- Original Equipment Manufacturer: Shall purchase a Lane Assistance System, that fits with the steering mechanism and uses indicator lamps as sensors. The OEM shall participate in the design aspects of the system as a whole to provide requirements and check on its coordination with other components. It shall check the functional safety aspects of the Lane Assist System with the rest of the vehicle

- Tier 1: Will produce the required Lane Assistance System. It shall be responsible for the proper functioning of the system and how each sub-system performs. It shall also see to the Functional Safety aspects of the system as a whole and as sub-systems
- Tier 2: Shall produce individual parts that shall be used to build the components of the sub-systems and systems that make the Lane Assistance System

Confirmation Measures

Confirmation measures serve the following:

- The Functional Safety conforms to ISO 26262
- The project establishes making a safer system

It establishes the same using a confirmation review, functional safety audit and functional safety assessment as follows:

- Confirmation Review: shall be carried out to check that the project agrees with the ISO 26262 standard for Functional Safety. An independent person shall carry out the review to check for compliance with the same
- Functional Safety Audit: shall be done to compare the actual implementation of the project with the Safety Plan so made. The audit shall be carried out by a person independent from the team creating the Safety Plan
- Functional Safety Assessment: shall be the final step that shall check if the Safety Plan and Functional Safety project actually achieve safety for the system

All confirmation measures shall be carried out by Independent teams/ individuals, separate from the team involved in design, documentation or implementation of the Safety project. Based on the document under review, different levels of Independence shall be deemed appropriate.

With this, we complete the initial stage, the Safety Plan, of the Functional Safety project.