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
2017-10-15	1.0	Albert Killer	First draft of safety plan

Table of Contents

Introduction

Purpose of the Safety Plan

The safety plan gives an overview of how to achieve a safe system. Among others this includes to define the system under consideration and to set up a goal for the project. Determine the steps that will be taken to ensure safety and appoint roles and personnel involved in the project. The project timeline sets deadlines and milestones to successfully implement the project in time.

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 investigated in this project is a *Lane assistance system*. The item's *lane departure warning function* vibrates the steering wheel in case the car drifts towards the edge of the lane. The item's l*ane keeping assistance function* moves the steering wheel so that the car turns back towards the center of the lane.
A drift from the lane center is detected by the car's *camera sensor* subsystem. The *electronic power steering ECU* subsystem takes inputs from the *camera sensor* subsystem and the *driver steering torque* subsystem and outputs to a *motor* providing torque to the steering wheel. In addition a *car display* subsystem provides visual feedback for the driver. All these subsystems are part of the item. The *steering wheel* itself is not part of the item and thus not part of this project.

Goals and Measures

Goals

The major goal of this project is to assure safe and reliable operation of the E/E/PS components of a vehicle's lane assistance function, according to ISO 26262. The lane assistance function consists of *lane departure warning* and *lane keeping assistance*. To achieve functional safety we are going to identfy hazards, measrure risks and finally apply systems engineering in order to lower risk to a reasonable level.

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	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

Although cost and productivty are important for a successful system and market integration, safety is our number one priority. Meeting funtional safety standards on a regular basis is going to be rewarded whereas undermining essential safety requirements in favor of timelines or costs is never an option and will be penalized. Designing functional safety is following defined processes and assures that design decisions are traceable back to the people and teams who made the decisions. Development and auditing teams are indepent and have to involve people of different of intellectual backgrounds. It is crucial that communication between those teams is based on full disclosure of problems. All necessary resources including people with appropriate skills are assigned to this functional safety project.

Safety Lifecycle Tailoring

When dealing with a new implementation and not modification, the entire safety lifecycle including all the phases mentiond in chapter **Scope of the Project** have to be to followed and documented. Hardware components and respective product development, as well as the final production and operations phase are part of another teams functional safety analysis and hence not part of this project.

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 purpose of the development interface agreement (DIA) is to delineate the roles and responsibilities between OEM and tier-1 involved in developing this product. Both parties 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 OEM provides a functioning lane assistance system. Tier-1 is going to analyze and modify various sub-systems according to functional safety requirements.

The following steps are part of a separate DIA documentation which will be attached to this safety plan:

- Appointment of customer and supplier safety managers
- Joint tailoring of the safety lifecycle
- Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
- Information and work products to be exchanged
- Parties or persons responsible for each activity in design and production
- Any supporting processes or tools to ensure compatibility between customer and supplier technologies

Confirmation Measures

Confirmation measures ensure that the applied processes comply with functional safety standards provided by ISO 26262 and that project execution is following the safety plan, therefore verifying if the design really does improve safety.

In particular by providing *confirmation review,* during design and development of the product, complience with ISO 26262 is assured by an independent person.

A *functional safety audit* checks that the actual implementation of the project considers the safety plan.

Finally *functional saftey assessment* confirms that plans, designs and developd products actually achieve functional safety.