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
2019-01-16	1.0		First draft

Table of Contents

Table of Contents

Introduction

Purpose of the Safety Plan

A safety plan documents how the functional safety is ensured by the company. Documenting the processes and steps of the development ensures the usage of best practices. It also contains documentation about what was changed in order to reduce the risk to acceptable levels.

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 helps the driver to stay in a lane. It consists of a lane departure warning and a lane assistance.

The lane departure warning senses the lane with a camera and vibrates the steering wheel, if the car is going to leave the current lane without any turn signal active. If the driver does not have any turn signal on and drives over a lane boundary, the system considers this case as unwanted by the driver and warns him by vibrating the steering wheel.

The lane assistance tries to keep the car in the middle of the lane. If the car goes outside the middle of the lane, it applies torque to the steering wheel in order to steer the car back to the middle of the lane. If the driver seems to be inactive (not having its hands on the steering wheel) the system will turn inactive as well, because the driver must always have the control over the car. If the system turns inactive because of the driver being absence it indicates this by an acoustic signal.

The system consists of the camera sensor and the camera sensor ECU for sensing the lane boundaries.
The car display ECU and the car display are used to display the status of the lane assistance system.
The driver steering torque sensor and the electronic power steering ECU are used to detect whether the driver has its hand on the steering wheel or not.
The electronic power steering ECU and the motor providing torque to the steering wheel are used to vibrate in case of a lane departure or to apply torque to the steering wheel in order to keep the car in the middle of the lane.
All the above-mentioned subsystems are included in the safety plan, except for the steering wheel.

Goals and Measures

Goals

Analyze the lane assistance functions with ISO 26262 and identify potential safety problems and handle them as appropriate, so that we have a product in the end, which is considered safe (the risks are accepted by the people).

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

To ensure a good safety of our products every team member should always consider safety over any other things like deadlines, costs or productivity. So, if deadlines are missed because

of safety issues, this is considered better than holding the deadline, but having still some safety issues open.
To motivate the team, one will get a gratification if he found a safety problem. The gratification will be doubled if he also has a realizable solution. The process for fault reporting needs to be considered.
Before the project begins the project manager analyzes how many engineers will need to carry out the project. One or more project teams will be created.
In meetings where the safety concept is discussed, a protocol is written, where the decisions are written down and who (based on meeting participants and meeting leader) made the decision.
A document management system (SharePoint) is used to track changes in documents.
Each software change needs to be started by creating an issue on our own GitLab server. The software engineer doing that change in the code needs to sign the changes he made using a GPG key (inside git) and then upload those changes to the GitLab server. This allows us to track all changes of a software project. While the engineer changes parts of the code, he also needs to create a separate unit test for his change. This ensures that the changes he made have the results he would expect. This is not the final test, because a separate team will do software unit tests independently from the department/team who is responsible for including the new functionalities in the software.
If a software engineer has questions on a software change request, he can open the issue on GitLab and see who created this request and can directly ask questions to him within the issue on GitLab. This also documents the changes and who made which decisions.
The testing is outsourced to another company and therefore independent from the team who developed the part.

Safety Lifecycle Tailoring

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

- Concept phase
  - Item definition
  - Initiation of safety lifecycle
  - Hazard analysis and risk assessment
  - Functional safety concept
- Product Development at the System Level
  - Product Development at the Software Level
  - Safety validation
  - Functional safety assessment
  - Release for production

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 purpose of this section is to define the which companies are involved in this product. And clarify between companies who is responsible for what part of the development. In case of a problem you can look here to find the party who can fix it.

The safety manager from the OEM is: ???
The safety manager from the Tier 1 is: ???

The OEM is responsible for providing documentation about the lane assistance system. It provides architectural as well as functional designs.
The Tier 1 analyzes the product and its subsystems for functional safety. It gives these reports back to the OEM, which needs to fix the critical/negative points.
If there are no critical points anymore in the design, the project moves on to the next step: testing.
For the testing phase the OEM also provides the devices which should be tested and also how they should be tested, to fulfill functional safety.
The Tier 1 is then responsible for creating a testing environment and carrying out the test.

Confirmation Measures

The functional safety project conforms to ISO 26262 and the project really does improve the safety of the vehicle.
The review must be carried out by an independent person, which has not designed or developed the project. This ensures the compatibility with ISO 26262.
The functional safety audit looks at the actual implementation and compares it to the safety plan and ensures they are equal.

The functional safety assessment ensures, that the project overall (plans, designs and development) confirms to ISO 26262 and makes the vehicle safer.