Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [1.0]
Template Version 1.0, Released on 2018-05-24

Document history

[Instructions: Fill in the date, version and description fields. You can fill out the Editor field with your name if you want to do so. Keep track of your editing as if this were a real world project.

For example, if this were your first draft or first submission, you might say version 1.0. If this is a second submission attempt, then you'd add a second line with a new date and version 2.0]

Date	Version	Editor	Description
22/05/2018	1.0	Aman Gupta	Initial Version

Table of Contents

[Instructions: We have provided a table of contents. If the table of contents is not showing up correctly in your word processor of choice, please update it. The table of contents should show each section of the document and page numbers or links. Most word processors can do this for you. In Google Docs, you can use headings for each section and then go to Insert > Table of Contents. Microsoft Word has similar capabilities]

Introduction

Purpose of the Safety Plan

The purpose of the plan is to provide an overall framework for the lane assistance functional safety project as pertain to the potential malfunctions of the electrical and electronic systems as defined by ISO 26262 standard, tailored.

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:

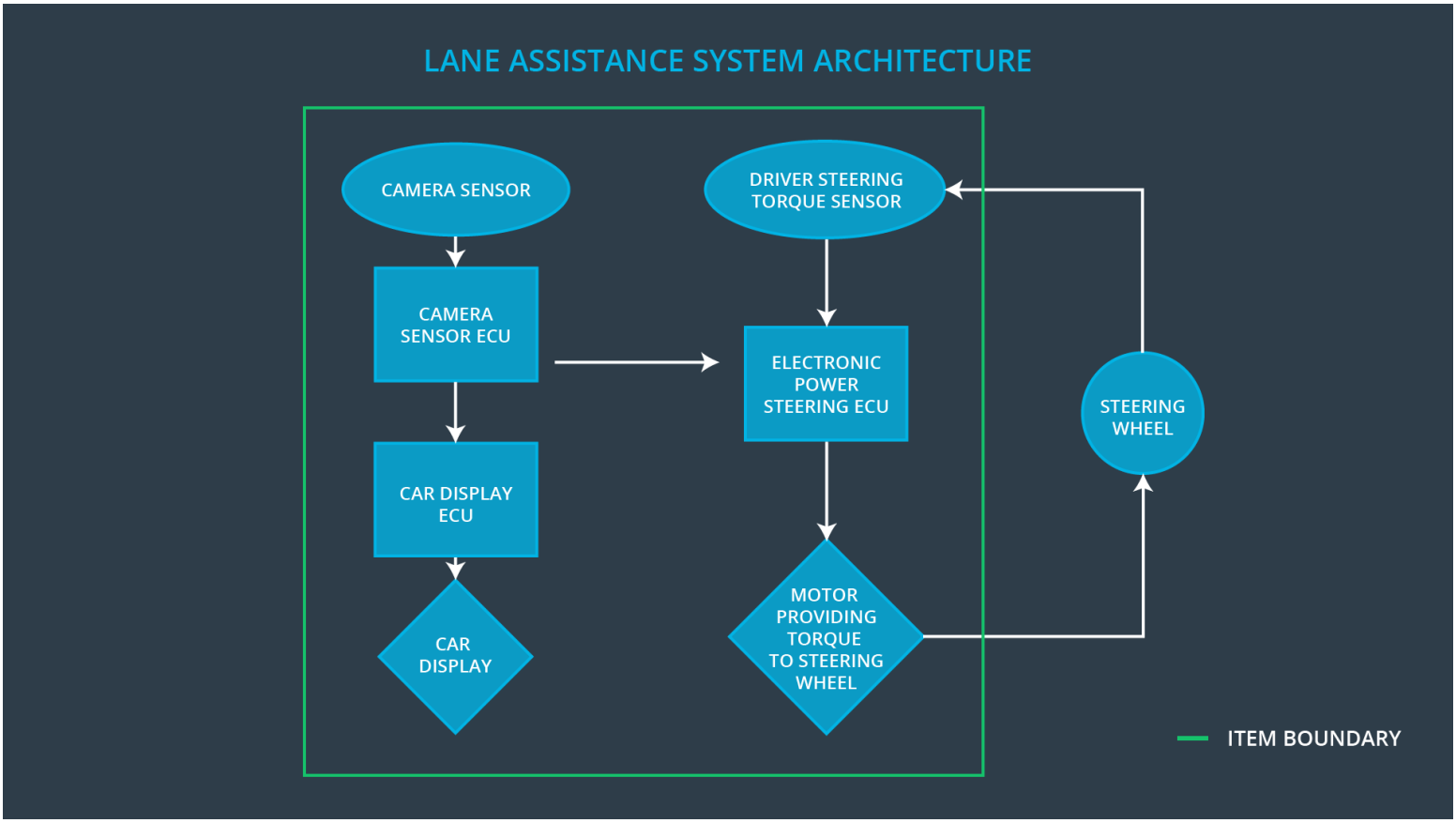
- Product Development at the Hardware Level
- Production and Operation

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 in this plan is Lane Assistance system ,which is a simplified version of an Advanced Driver Assistance System (ADAS) that warns the driver of unintended steering drifts and assists the driver in steering back to the center of the lane.

The two main functions of Lane Assistance items are:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane when this item is engaged, two things will happen:

1. The **lane departure warning function** shall apply an oscillating steering torque to provide the driver a haptic feedback (vibration).

2. The **lane keeping assistance function** shall apply the steering torque when active in order to stay in ego (current active) lane.

Subsystems:

- Camera subsystem: monitors the lane line and generate torque requests
- Electronic power steering subsystem: provides the final torque to the steering wheel
- Display system: displays the warning message to the driver

The only subsystem outside the item boundary is the steering wheel itself. The rest of 3 subsystems mentioned above are all inside.

The camera system detects lane departures and tells the steering wheel how hard to turn. The driver receives a warning on the vehicle display and also receives a warning via a steering wheel vibrating. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane.

Goals and Measures

Goals

This project goals are:

- Distinguish hazardous and risky circumstances in the electronic Line Assistance system making injuries to a person.
- Evaluate the risks related to the hazardous situations.
- Lower the risk of the malfunctions to levels acceptable by society.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	Entire team	Constantly
Create and sustain a safety culture	Safety Manager	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

Some features of the safety culture in our company:

- **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

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

A DIA (development interface agreement) defines the roles and responsibilities between companies involved in developing a product. 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.

- **Functional Safety Manager - Item Level**: Pre-audits, plans the development phase for the project.

- **Functional Safety Engineer - Item Level**: Develop prototypes, integrate subsystems combining them into the larger complete Lane Assistance item.

- **Project Manager - Item Level**: Allocates the resources needed for the project.

- **Functional Safety Manager - Component Level**: Pre-audits, plan the development phase for the inner components used in the project.

- **Functional Safety Engineer - Component Level**: Develop prototypes and integrate components conforming the Lane Assistance item.

- **Functional Safety Auditor**: Make sure the project conforms to the safety plan.

- **Functional Safety Assessor**: Judges whether the final solution has increased levels of safety from the previous state.

Confirmation Measures

The Confirmation Measures serve the following two purposes:

- The Lane Assistance safety project conforms to ISO 26262 tailored

- The Lane Assistance safety project does make the vehicle safer.

The **Confirmation review** will ensure that the safety project complies with ISO 26262 as tailored by an independent appointed safety auditor. The **Functional Safety Audit** will ensure that the actual implementation of he project conforms to the safety plan by an independent appointed safety auditor. The Functional Safety assessment will ensure that plans, designs and developed products actually achieve functional safety by an independent appointed safety 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.