Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: version 1.0

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
29/10/2017	1.0	Adriana Costas	First attempt

Table of Contents

Roles

Development Interface Agreement

Confirmation Measures

Introduction

Purpose of the Safety Plan

The purpose of this safety plan is to provide an overall framework for the Lane Assistance item, an to assign roles and responsabilities for functional safety for this item.

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 item alerts the driver that the vehicle has accidentally departed its lane and attempts to steer the vehicle back toward the center of the lane.

The Lane Assistance system will have two functions:

1. Lane departure warning: it shall apply an oscillating steering torque to provide the driver a haptic feedback.
2. Lane keeping assistance: it shall apply the steering torque when active in order to stay in ego lane.

The item boundary include three subsystems as shown in Figure 1 :

1. Camera system
2. Electronic Power Steering system
3. Car display system

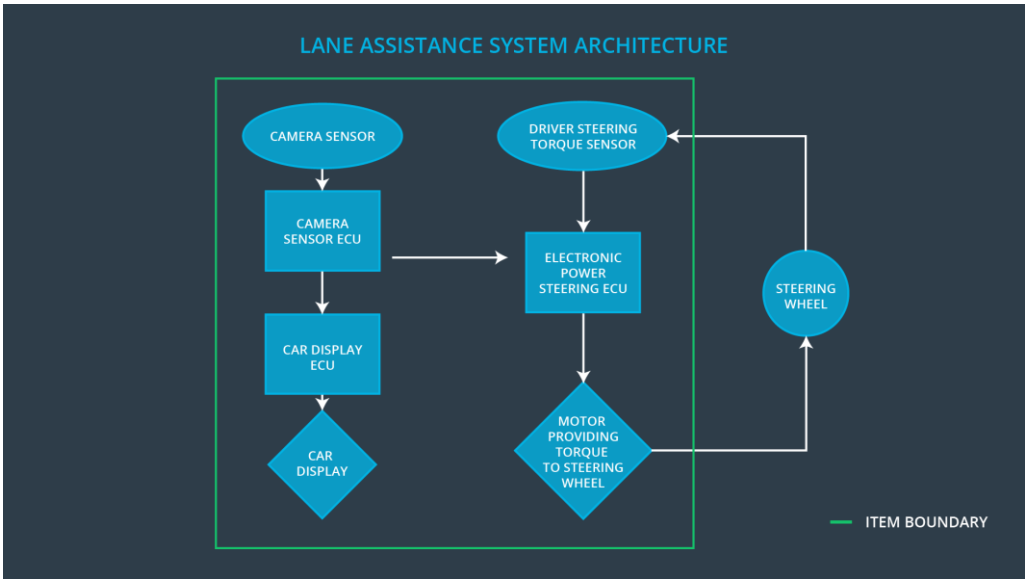

Figure 1 Lane Assistance System Architecture

Goals and Measures

Goals

The goals of the Lane Assitance Functional Safety Plan for the project are:

- Indentifying risk hazardous situations in a lane assitance electronic or electric system malfunction that may cause physical injury or damage to a person's health.
- Evaluate the risk level of the hazardous situation.
- Via systems engineering, lowering high risk level situations to reasonable levels to prevent accidents from ocurring.

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 assesor	Conclusion of functional safety activities

Safety Culture

Here are some characteristics of a our safety culture:

- 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 functional safety initial plan, the ISO 26262 standard have been tailored to include the following safety lifecycle phases 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 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 a development interface agreement (DIA) is to define the roles and responsabilities 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.

In the line below, we specify the responsabilities of each role:

- Project Manager – Item Level (OEM): Item level resources allocation with adequate functional competency, and appointment of external Functional Safety Auditor and Assesor. Lane Assistance system functional safety plan, and confirmation measures acceptance.
- Tier-1 Project Manager: component level resources allocation with adequate functional safety competency.

- OEM Functional Safety Manager/Engineer: coordinate and document the item level planned safety activities including concept phase and product development at the system and software level. Perform functional safety pre-assesment prior to audit by external functional safety assessor three months prior ot main assessment.
- Tier-1 Safety Manager: Joint tailoring of the safety lifecycle.
- All OEM, Tier-1 and their selected suppliers team members: Follow safety processes and create and sustain a safety culture as indentified in section about Safety Culture of this plan.
- Tier-1 Safety Manager/Engineer: coordinate and document the component level planned safety activities including concept phase and product development at the component and subsytem software level in compliance with item level planned and safety activities as developed by OEM Functional Safety Manager/Engineer.
- Safety Auditor: Plan the safety activities of the safety lifecycle once every two months.
- Safety Assessor: perform functional safety assessment at conclusion of functional safety activities.

Confirmation Measures

Confirmation measures serve two purposes:

- that a functional safety project conforms to ISO 26262, and
- that the project really does make the vehicle safer.

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

A confirmation review is a review that ensures that the project complies with ISO 26262. As the product is designed and developed, an independent person would review the work to make sure ISO26262 is being followed.

A functional safety audit is the process that checks that the actual implementation of the project conforms to the safety plan whereas a functional safety assessment confirm that plans, designs and developed products actually achieve functional safety.

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.