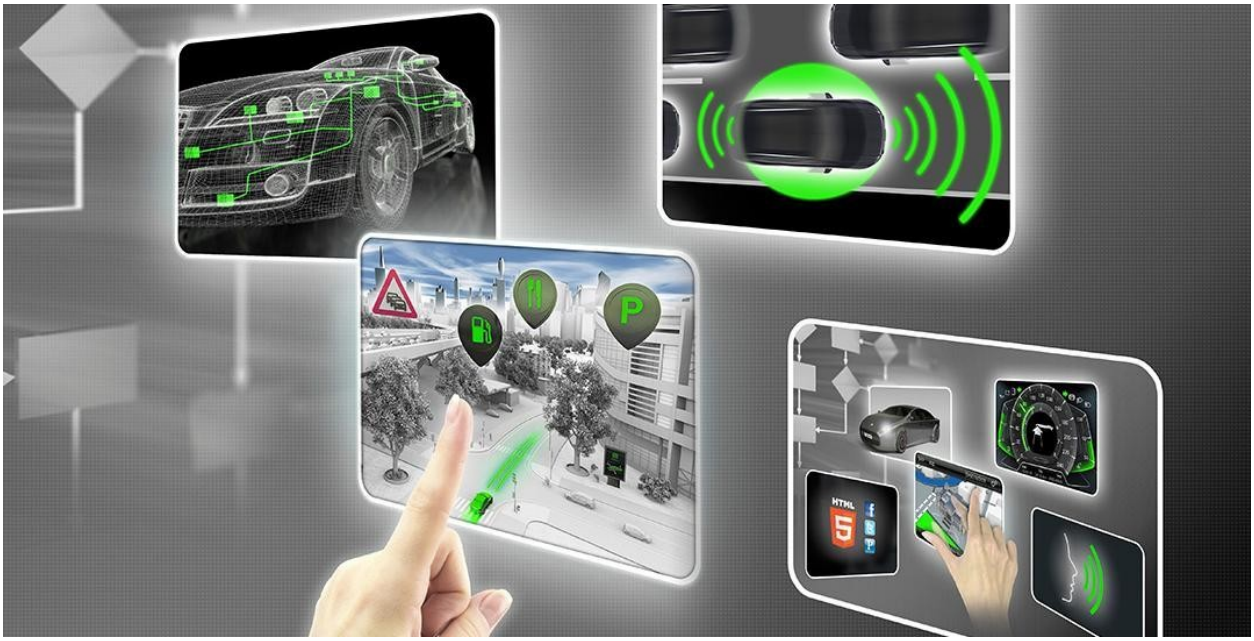
Elektrobit

UDACITY

Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



Document history

Date	Version	Editor	Description
31.05.2018	1.1	Ankith Manjunath	Safety Plan for Lane assistance

Table of Contents

Introduction

Purpose of the Safety Plan

Safety plan documents the use case and the roles and responsibilities of carrying out a safety analysis for a E/E system according to ISO 26262 specifications. It also includes task needed to be performed and tracks the schedule of the associated tasks. The end product is a document stating a particular system under development has been designed in a way to be safe and reduce the impact of a hazard if occurs.

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 system under test is the Lane assistance system. Lane assistance system includes two main functionalities namely

- Lane keep assist:- When the driver drift out toward the edge of the lane, this functionality will move the steering wheel so that the wheels turn toward the center of the lane.
- Lane departure warning :- When the driver drift out toward the edge of the lane, the steering wheel vibrates to warn the driver.

The item functionalities are implemented by the following subsystem:

- **Camera subsystem**: This subsystem includes following components:
  - Camera sensor
  - Camera sensor ECU (Electronic Control Unit)
- **Electronic Power Steering subsystem**: This subsystem is composed by three components:
  - Driver Steering Torque Sensor.
  - Electronic Power Steering ECU.
  - Motor Proving Torque to Steering Wheel.
- **Car Display subsystem**: This subsystem is composed by two components:
  - Car Display ECU
  - Car Display

The Line Assistance System does not include the following functionalities:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring

Goals and Measures

Goals

The goal of the current document is to document a safety plan for a lane assistance system to adhere with ISO 26262 standards and make the system functionally safe for release into public roads.

Measures

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team members	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

The compancy safety culture has the following points

- **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
- **High priority**: safety has the highest priority among competing constraints like cost and productivity

Safety Lifecycle Tailoring

The scope of the safety concept and its life cycle

- Concept phase
- Product development at the system level
- Product development at the software level

The safety lifecycle does not inlude the

- Product development at the hardware level

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

1. What is the purpose of a development interface agreement?
   Clearly defines the roles and responsiblities assigned to between various teams within or outside the company. The DIA also helps in keeping a record of performed tasks so in case of a malfunction or a recall, appropriate teams can be notified and issues could be fixed faster.

2. What will be the responsibilities of your company versus the responsibilities of the OEM? Hint: In this project, the OEM is supplying a functioning lane assistance system. Your company needs to analyze and modify the various sub-systems from a functional safety viewpoint.
   Being a tier 1 company the responsiblities include developing a functionally safe system (e.g Lane assitance system) as per the requirements of the OEM.
   OEM resposibilites include using the developed function and to integrate into the vehicle system and testing the complete vehicle system along with the developed sub system is functionally safe.

Confirmation Measures

1. **What is the main purpose of confirmation measures?**
   Confirmation measures takes care whether the development process adheres to the safety plan development during the concept phsae and also checks how close the project progress with the functional safety plan.
2. **What is a confirmation review?**
   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 ISO 26262 is being followed.

3. **What is a functional safety audit?**
   Checking to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit.

4. **What is a functional safety assessment?**
   Confirming that plans, designs and developed products actually achieve functional safety is called a functional safety assessment.

]

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.