



Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21



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
20 June 2019	1.1	Guilin Zhu	

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]

[Document history](#)

[Table of Contents](#)

[Introduction](#)

[Purpose of the Safety Plan](#)

[Scope of the Project](#)

[Deliverables of the Project](#)

[Item Definition](#)

[Goals and Measures](#)

[Goals](#)

[Measures](#)

[Safety Culture](#)

[Safety Lifecycle Tailoring](#)

[Roles](#)

[Development Interface Agreement](#)

[Confirmation Measures](#)

Introduction

Purpose of the Safety Plan

[Instructions: Answer what is the purpose of a safety plan?]

The safety plan is a living document for planning, coordination and documentation of safety activities, which include safety lifecycle, safety management roles and responsibilities, DIA as well as confirmation measures.

The main purpose of this work product serves to systematically plan and allocate the safety activities required and the resources necessary for its implementation, and safety plan also forms the basis for the creation of “Safety Cases”, a systematic summary of all documents necessary for proving functional safety against ISO26262.

Scope of the Project

[Instructions: Nothing to do here. This is for your information.]

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

[Instructions: Nothing to do here. This is for your information.]

The deliverables of the project are:

- Safety Plan
- Hazard Analysis and Risk Assessment
- Functional Safety Concept
- Technical Safety Concept

Item Definition

[Instructions:

REQUIRED

Discuss these key points about the system:

What is the item in question, and what does the item do?

What are its two main functions? How do they work?

Which subsystems are responsible for each function?

What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?

An item refers to a high level system in the vehicle system, which describes the functional concept of the product, as well as what happens when the system malfunctions.

Lane assistance system is the item in this project, which consists of lane departure warning function and lane keeping assistance function. Lane departure warning function will provide vibration warning to the steering wheel so that driver is able to be well-informed and alerted. The lane keeping assistance function will assist the driver always maintain the vehicle at the center of lane, in other words, the function will provide additional steering effort if necessary when vehicle deviates the center of lane.

The figure 1 below shows the lane assistance system architecture which consists of camera subsystem, car display subsystem, electric power steering subsystem.

Car display subsystem, camera subsystem as well as EPS system are responsible for lane departure warning function, and all subsystems except car display subsystem are responsible for lane keeping assistance system.

As described in the figure 1 below, all car display, camera system as well as EPS are inside the items, and steering wheel is outside of the item.

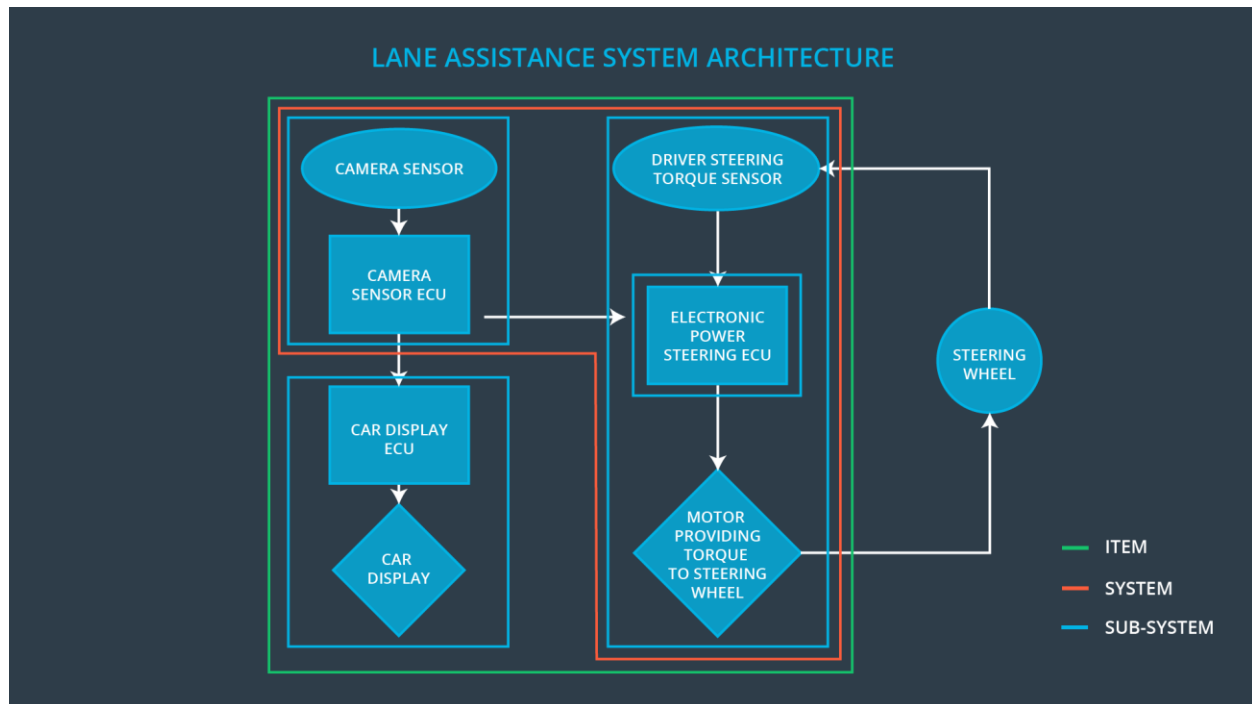


Figure 1 The Lane Assistance System Architecture

OPTIONAL

Optionally, include information about these points as well. These were not included in the lectures, but you might be able to find this information online:

- Operational and Environmental Constraints. This could especially be limited to camera performance; lane lines are difficult to detect in snow, fog, etc
- Legal requirements in your country for lane assistance technology
- National and International Standards Related to the Item
- Records of previously known safety-related incidents or behavioral shortfalls

Goals and Measures

Goals

[Instructions:

Describe the major goal of this project; what are we trying to accomplish by analyzing the lane assistance functions with ISO 26262?]

The goal of this project is to analyze the potential hazards and failures/malfunctions that system may have and add extra safety requirements to ensure the functional safety and make sure that the product/function comply with ISO26262.

Measures

[Instructions:

Fill in who will be responsible for each measure or activity. Hint: The lesson on Safety Management Roles and Responsibilities.

The options are:

All Team Members

Safety Manager

Project Manager

Safety Auditor

Safety Assessor

]

Measures and Activities	Responsibility	Timeline
Follow safety processes	Safety Manager	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

[Instructions:

Describe the characteristics of your company's safety culture. How do these characteristics help maintain your safety culture. Hint: See the lesson about Safety Culture

]

Safety is the highest priority in the product development, and process ensure accountability such that design decisions are traceable back to the people and teams who made the decisions.

Safety Lifecycle Tailoring

[Instructions:

Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the of this document

]

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

[Instructions:

This section is here for your reference. You do not need to do anything here. It is provided to help with filling out the development interface agreement section.

]

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

[Instructions:

Assume in this project that you work for the tier-1 organization as described in the above roles table. You are taking on the role of both the functional safety manager and functional safety engineer.

Please answer the following questions:

1. What is the purpose of a development interface agreement?

The purpose of development interface agreement is to define the roles and responsibilities between companies involved in developing a product. All involved parties need to agree on the contents of DIA before the project begins.

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.

]

The responsibility of our company is to derive the functional safety concept, safety requirements at system and software level.

Confirmation Measures

[Instructions:

Please answer the following questions:

1. What is the main purpose of confirmation measures?
2. What is a confirmation review?
3. What is a functional safety audit?
4. What is a functional safety assessment?

]

The confirmation measures serve two purposes:

1. a functional safety project conforms to ISO26262, and
2. the project really does make the vehicle safer

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.

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.

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.