



Elektrobit



UDACITY

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
2017-09-17	1.0	Sundeep Tuteja	Safety Plan – Lane Assistance

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 purpose of the safety plan is to provide an overview of how to achieve a safe system. It takes into account the system under consideration, the goal of the project, the steps that will be taken to ensure safety, the roles and personnel involved in the project, and the project timeline.

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
- Software Safety Requirements and Architecture

Item Definition

[Instructions:

REQUIRED

Discuss these key points about the system:

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

The item in question is the lane assistance system. It alerts a driver when a vehicle unintentionally departs the lane, and attempts to steer the vehicle back to the center of the lane.

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

The lane assistance system has two main functions:

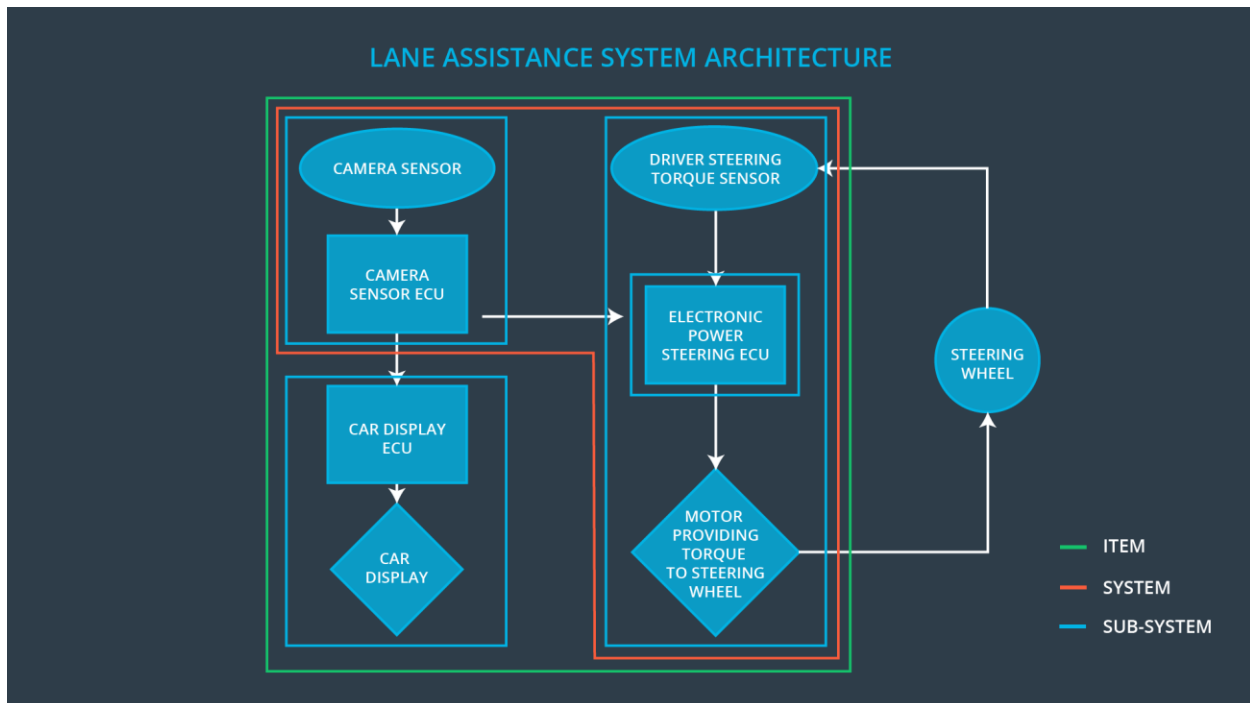
- Lane departure warning: The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback indicating that the vehicle is crossing a lane marker when it was not intended.
- Lane keeping assistance: The lane keeping assistance function will automatically turn the steering wheel to guide the vehicle towards the center of the ego lane, in order to avoid lane departure.

Which subsystems are responsible for each function?

The systems responsible for the lane departure warning and lane keeping assistance functions are:

- Camera subsystem
- Electronic Power Steering subsystem
- Car display subsystem

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



The above figure shows the boundaries of the lane assistance item, along with the camera subsystem, electronic power steering subsystem, and car display subsystem that are inside the lane assistance item. It also shows that the steering wheel is the only element that is outside the boundary of the item.

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 major goals of analyzing the lane assistance item with ISO26262 are as follows:

- **Identification of hazards** that could cause physical injury or damage to a person's health
- **Evaluation of risk** of potential hazardous situations so that we know how much we need to lower the risk
- **Prevention of accidents** via systems engineering by lowering risk to reasonable levels

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	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	Project Manager	Within 2 weeks of start of project

functional safety competency		
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

]

- **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 are independent from the teams who audit the work
- **Well defined processes:** Company design and management processes are clearly defined
- **Resources:** Projects have the 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

[Instructions:

Describe which phases of the safety lifecycle are in scope and which are out of scope for this particular project. Hint: See the [Intro section](#) 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?

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.

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.

OEM: OEM shall be responsible for the following activities

- Appointment of a customer safety manager
- Active participation in all phases of the safety lifecycle
- Development of high level safety requirements
- Furnishing of technical information as needed
- Appointment of a safety assessor and a safety auditor

Supplier: Supplier shall be responsible for the following

- Appointment of a supplier safety manager
- Active participation in all phases of the safety lifecycle
- Development of safety plan, Hazard and Risk Assessment, Functional Safety Concept, Technical Safety Concept, and Software Requirements

]

Confirmation Measures

[Instructions:

Please answer the following questions:

1. What is the main purpose of confirmation measures?

Confirmation measures serve two main purposes:

- Ensuring that the functional safety project conforms to ISO26262
- Ensuring that application of ISO26262 actually increases vehicle safety
- 2. **What is a confirmation review?**
A confirmation review involves ensuring that the project complies with ISO26262
- 3. **What is a functional safety audit?**
This involves checking to make sure that the actual implementation of the project conforms to the safety plan
- 4. **What is a functional safety assessment?**
This involves confirming 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.