



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
04/11/2018	1.0	Oyama	First Attempt
04/12/2018	2.0	Oyama	Minor changes at DEVELOPMENT INTERFACE AGREEMENT

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 overall framework for the Lane Assistance item, and to assign roles and responsibilities for functional safety for this item.

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?

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?

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

]

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.

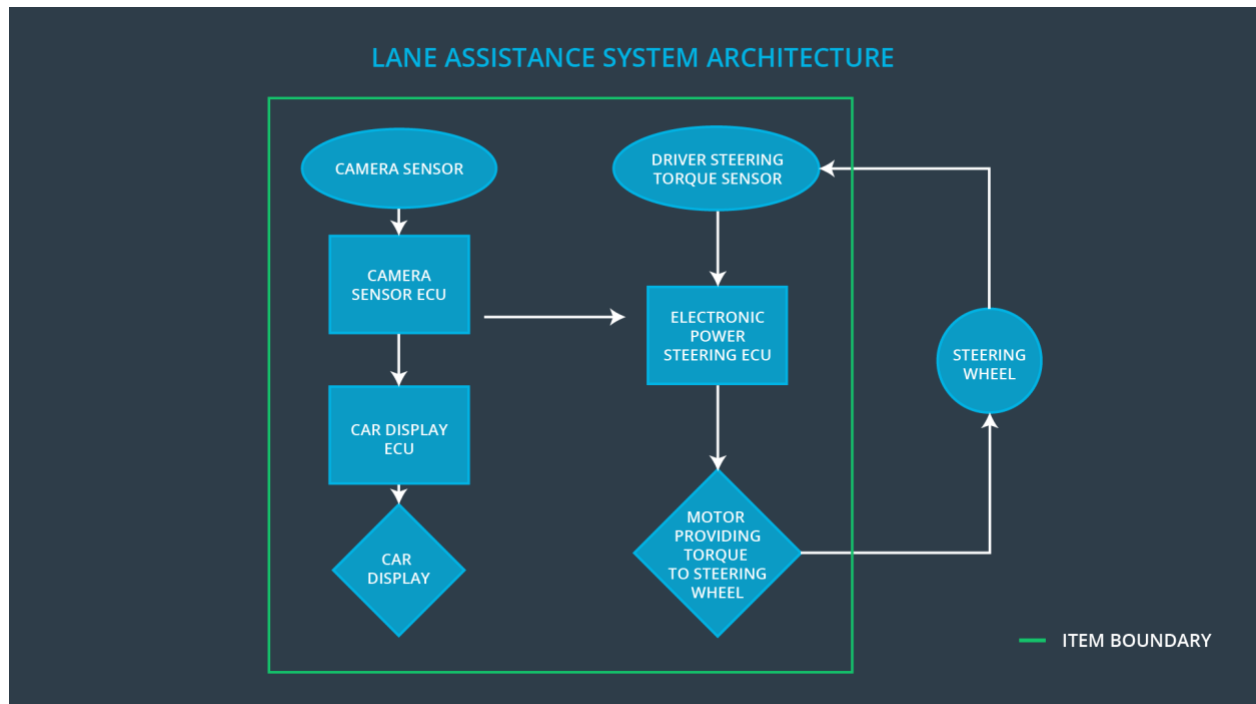
The Lane Assistance System will have two functions:

1. Lane departure warning
2. Lane Keeping Assistance

The lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback.

The lane keeping assistance function shall apply the steering torque when active to stay in ego lane.

The camera subsystem, the electronic power steering subsystem, and the car display system are each responsible for each of the functions.



- (1) Camera system is responsible for detecting lane lines and determining when the vehicle leaves the lane by mistake.
- (2) Electronic Power Steering system is responsible for the torque provided by the driver and then adding an appropriate amount of torque based on a lane assistance system torque request.
- (3) Car Display system is responsible for the alert to the driver when the vehicle leaves the lane by mistake.

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 ISO 26262 functional safety standard covers electronic and electrical malfunctions in passenger vehicle systems. The standard provides a framework for reducing risks that could harm people's health. In ISO26262 functional safety, these are the four main steps involved in functional safety according to the standard:

- (1) Requirements engineering Define what the system is going to do
- (2) Designing or modifying a system architecture Design what the system will look like
- (3) Test the system to make sure it behaves as expected
- (4) Integrate the system into larger systems

By analyzing the lane assistance functions with ISO 26262, we can get the details for each step above, make a plan to reduce risks, and after this step, we can move forward to the right side of the V model, which involves implementing the plans and designs through software and hardware engineering. Implementations also need to be tested to make sure that they follow the design specifications from the left side of the V.

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	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

]

Our company's safety culture is regarding processes and accountabilities for each process as very important. Each process is also required to be documented well, and will be got heavy penalties unless the documentation. On the other hand, our companies consists of many staffs who belong to our company for long term, so we have tendency toward lacking of intellectual diversity.

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?
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.

]

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.

Tier-1 will be responsible for complying with the requirements for building up the organizations as well as to satisfy the functional safety of our component. In addition, its process, operations, appointing persons in charge, and necessary tools to cooperate with OEM.

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 purpose of Confirmation Measures includes 2 items. One is that a functional safety project conforms to ISO 26262, and the 2nd is that the project really does make the vehicle safer.

By confirmation review, we check it 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.

Also, Functional safety audit checks to make sure that the actual implementation of the project conforms to the safety plan is called a functional safety audit. And Functional safety assessment confirms that plans, designs and developed products actually achieve functional safety.

On the other hand, a person who develops a system that is rated low risk can be on the same team as the person who reviews the system for ISO 26262 compliance.

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.