

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 |
| 23/9/2018 | 1.0 | Flash yuan | First attempt |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 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](https://support.google.com/docs/answer/116338?co=GENIE.Platform%3DDesktop&hl=en), you can use headings for each section and then go to Insert > Table of Contents. [Microsoft Word](https://support.microsoft.com/en-us/help/285059/how-to-create-a-table-of-contents-by-marking-text-in-word) has similar capabilities]**

[Document history](#_1t3h5sf)

[Table of Contents](#_ktt3lgighckp)

[Introduction](#_zakt536q9xt3)

[Purpose of the Safety Plan](#_52ybytyytfvs)

[Scope of the Project](#_sh22j99mm02k)

[Deliverables of the Project](#_fzzlhwsfq6ys)

[Item Definition](#_t6m96u2v69wo)

[Goals and Measures](#_km1cu1hyl182)

[Goals](#_ww7fqc274i9y)

[Measures](#_v2rbrzjrkt9b)

[Safety Culture](#_b23s6orj91gm)

[Safety Lifecycle Tailoring](#_pqn9poe0nvtc)

[Roles](#_xlicd1ijavb7)

[Development Interface Agreement](#_swj0emygbhrm)

[Confirmation Measures](#_lllavvxrxrdy)

# Introduction

## Purpose of the Safety Plan

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

Safety Plan helps to build stable systems and avoid most risks in real cases. It provides testing evidence that shows system function.

## 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 System will have two functions:

1. Lane departure warning
2. Lane keeping assistance

When the driver drifts towards the edge of the lane, two things will happen:

* the ****lane departure warning function**** will vibrate the steering wheel
* the ****lane keeping assistance function**** will move the steering wheel so that the wheels turn towards the center of the lane

To state the ****lane departure warning**** engineering requirement more formally: "the lane departure warning function shall apply an oscillating steering torque to provide the driver a haptic feedback." In other words, the vehicle quickly moves the steering wheel back and forth to create a vibration. You can assume that the engineering requirement came from a product engineering team, and your job will be to add extra requirements to ensure functional safety.

The ****lane keeping assistance functionality**** will automatically ****assist**** the driver; the steering wheel turns towards the center of the lane. We will formally list the requirement as "the lane keeping assistance function shall apply the steering torque when active in order to stay in ego lane". Ego lane refers to the lane in which the vehicle currently drives.

When the camera senses that the vehicle is leaving the lane, the camera sends a signal to the electronic power steering system asking to turn and vibrate the steering wheel.

The camera sensor will also request that a warning light turn on in the car display dashboard. That way the driver knows that the lane assistance system is active.

What if the driver wants to leave the lane? If the driver uses a turn signal, then the lane assistance system deactivates so that the vehicle can leave the lane. The driver can also turn off the system completely with a button on the dashboard.

The driver is still expected to have both hands on the steering wheel at all times. The electronic power steering subsystem has a sensor to detect how much the driver is already turning. The lane keeping assistance function will merely add the extra torque required to get the car back towards center. The extra torque is applied directly to the steering wheel via a motor.

### **Lane Assistance System Architecture**

Now we will look at what the system looks like from a bird's eye view. Take a look at this diagram of the system architecture.

An architecture is a block diagram of the main parts of a system. This high level overview allows us to see how the system works without yet needing to know the details of the hardware and software implementations.

ECU stands for Electronic Control Unit. An ECU is a small computer that contains the hardware and software for a specific vehicle functionality. The camera ECU, for example, might have the hardware and software required for deep learning or for computer vision techniques like the Hough transform.

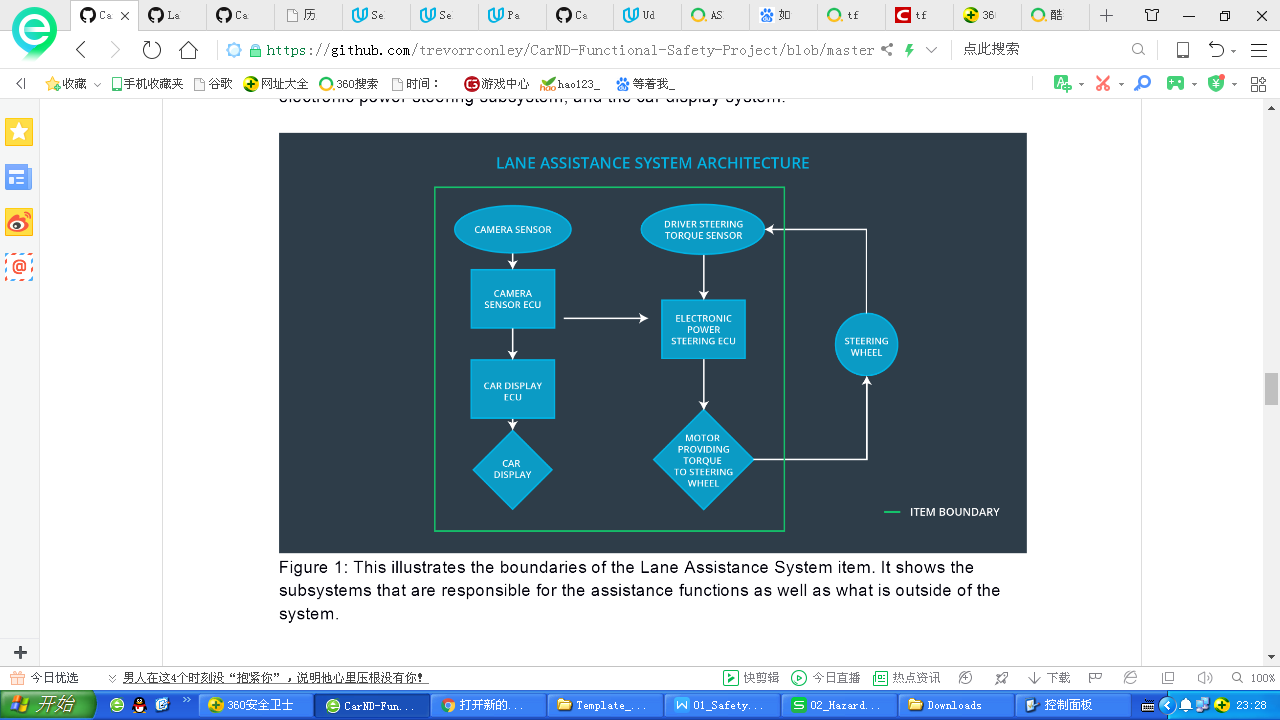
To summarize the functionality, the camera system detects lane departures and tells the steering wheel how hard to turn. The driver receives a warning on the vehicle display and also receives a warning via a steering wheel vibrating. Simultaneously, the wheel adds extra steering torque to help the driver move back towards the center of the lane.

### **Lane Assistance System: Sub System Architecture**

If we dig down further into the power steering ECU sub-system, we divide the ECU into its hardware and software components. We can further subdivide the software and hardware into components, parts, and units as shown in the diagram below. As we traverse down the V model, the architecture diagrams become more focused and detailed.

you can see that the item boundary was drawn to include three sub-systems:

* Camera system
* Electronic Power Steering system
* Car Display system



# 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?]**

ISO 26262 requires independent audits. The audits check if the project followed the steps outlined in the standard. Auditors will rely on the documentation to assess your work. An audit may be followed by a safety assessment, used to determine if the decisions made and steps taken achieve appropriate safety.

## 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 Assessor | 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**

**]**

### **Good Safety Culture**

Here are some characteristics of a good 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

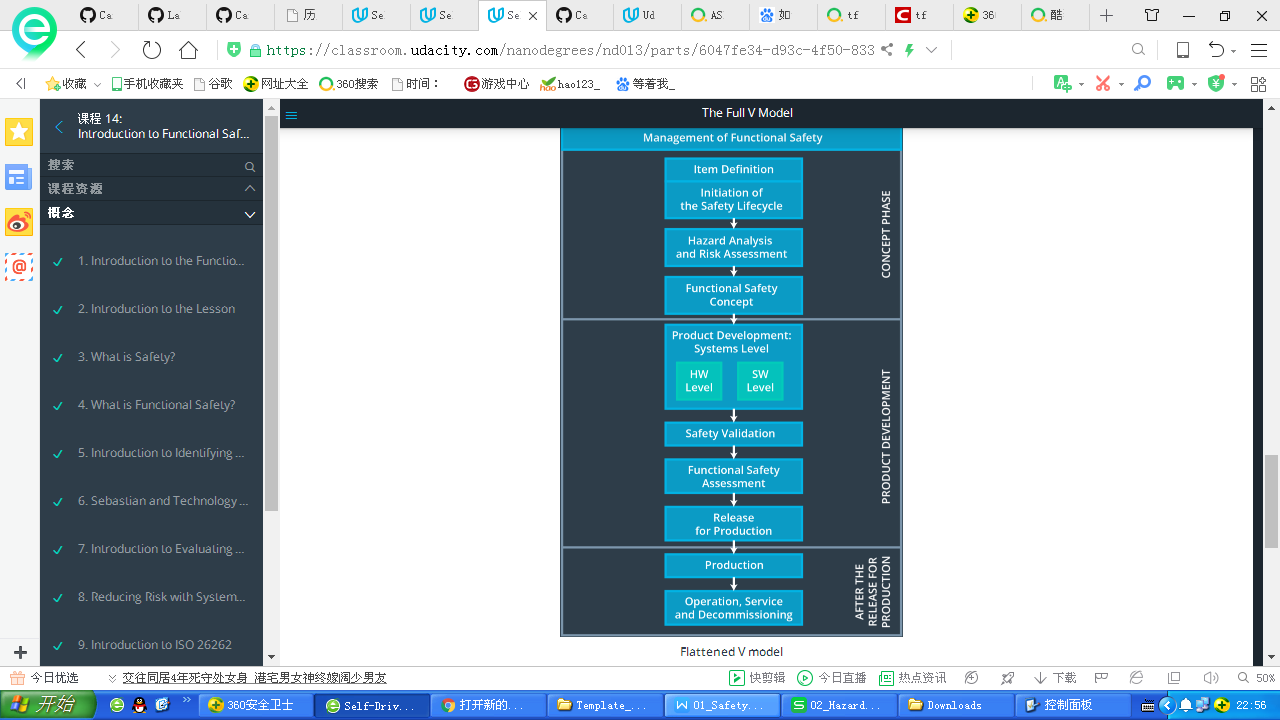
# Safety Lifecycle Tailoring

**[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](#_sh22j99mm02k) of this document**

**]**

1. old product, tailor lifecycle by needs.
2. New product , follow V model:



# 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.**

**]**

1)Project Manager

* Overall project management
* Acquires and allocates resources needed for the functional safety activities
* Appoints safety manager or might act as safety manager

2)Safety Manager

* Planning, coordinating and documenting of the development phase of the safety lifecycle
* Tailors the safety lifecycle
* Maintains the safety plan
* Monitors progress against the safety plan
* Performs pre-audits before the safety auditor

3)Safety Engineer

* Product development
* Integration
* Testing at the hardware, software and system levels

4)Safety Auditor

* Ensures that the design and production implementation conform to the safety plan and ISO 26262.
* Must be independent from the team developing the project

5)Safety Assessor

* Independent judgement as to whether functional safety is being achieved via a functional safety assessment
* Must be independent from the team developing the project

6)Test Manager

* Plans testing activities
* Coordinates testing to show that the vehicle system works correctly

These are the main management roles in the functional safety lifecycle; there would still be other people involved including requirement engineers, test engineers, hardware engineers, and software engineers.

|  |  |
| --- | --- |
| 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.

Here are major sections of a DIA:

* Appointment of customer and supplier safety managers
* Joint tailoring of the safety lifecycle
* Activities and processes to be performed by the customer; activities and processes to be performed by the supplier
* Information and work products to be exchanged
* Parties or persons responsible for each activity in design and production
* Any supporting processes or tools to ensure compatibility between customer and supplier technologies

# 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?**

**]**

### **Confirmation Measures Definitions**

##### ***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.

You will not be required to write out a full confirmation measure section in the final project's safety plan; but you will need to show that you understand the purpose of the confirmation measures.

### **Levels of Independence**

The person who developed a document, plan, design or product should not be the same person who carries out a confirmation measure; confirmation measures require independence.

ISO 26262 requires different levels of independence depending on what part of the functional safety lifecycle is under review.

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.