



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-Aug-17	0.1	Raghu	Initial draft

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?]

Vehicles have a number of different systems including hydraulic, mechanical, electrical, electronic, and chemical. Functional safety is a part of overall automotive safety and specifically refers to reducing risks in electrical and electronic systems. It looks at what happens when the system does something that it was not supposed to do, which is called a malfunction. Functional safety standards for the automotive industry in systems engineering - ISO 26262, is used to methodically reduce risk in passenger vehicle's electric/electronic systems.

The safety plan forces the project team to define roles, then outline the steps that would be taken to achieve functional safety (absence of unreasonable risks).

The safety plan gives an overview of how you are going to achieve a safe system. A few of the major elements include:

- Description of the system under consideration
- Goal of the project
- High-level steps that would be taken to ensure safety
- Roles and personnel involved in the project
- Project timeline

As the project passes through the design, implementation, and production phases, the output will be checked against the safety plan.

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:

Advanced driver assistance systems (ADAS) constantly monitor the vehicle surroundings as well as the driving behavior to detect potentially dangerous situations at an early stage. In critical driving situations, ADAS systems has two functions.

- Alert the driver to potentially dangerous situations
- Take control over the vehicle to prevent accidents from occurring

Here are a few examples of ADAS systems that are found in passenger vehicles today:

- Adaptive Cruise Control
- Automatic Parking
- Blind Spot Monitoring
- Lane Departure Warning
- Lane Keeping Assistance
- Tire Pressure Monitoring
- Pedestrian Protection

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

Lane assistance item is the part of the vehicle under consideration.

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

A lane assistance item generally has two functions:

- 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

If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. The system will vibrate the steering (lane departure warning) and also move the steering wheel back towards the lane center (lane keeping assistance).

Which subsystems are responsible for each function?

Lane departure Warning

If a driver departs a lane without using a turn signal, the system assumes that the driver has become distracted and did not mean to leave the lane. 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. The system will vibrate the steering (lane departure warning).

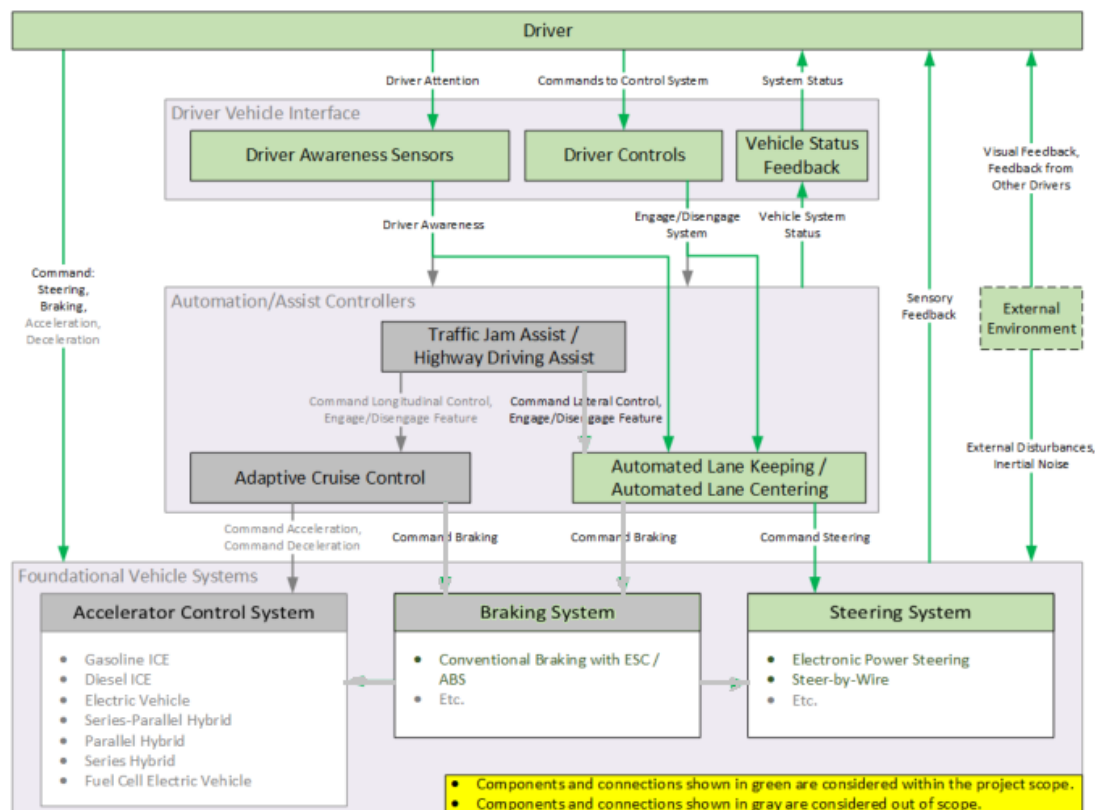
Lane Keeping Assistance

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. 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.

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.

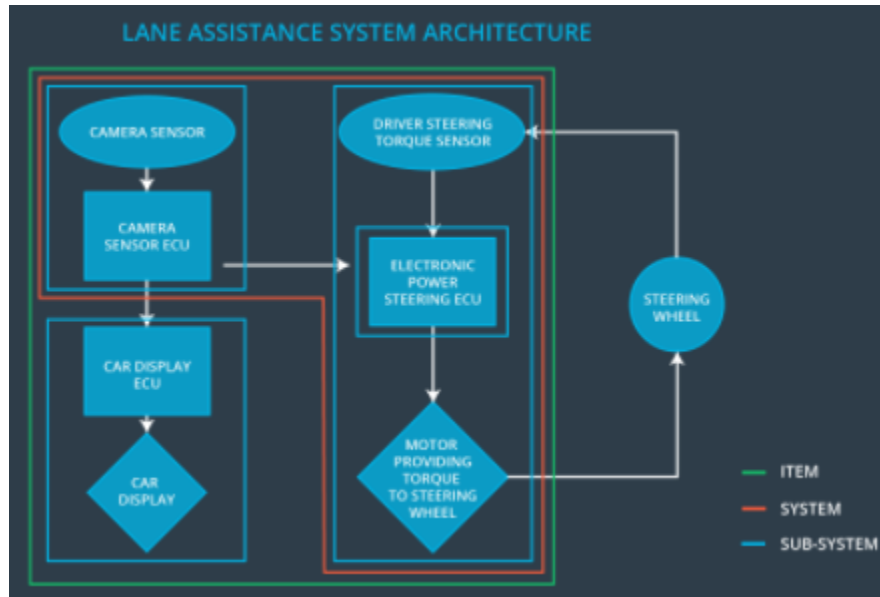
What are the boundaries of the item? What subsystems are inside the item? What elements or subsystems are outside of the item?

Boundary of the item



Source: US DOT Functional Safety Analysis of Automated Vehicle Lane Centering Control Systems.pdf

Systems / Subsystems inside the item



From the above diagram, item boundary includes three sub-systems:

- Camera system
- Electronic Power Steering system
- Car Display system

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 in functional safety is to avoid accidents by reducing risks to acceptable levels. This is done by,

1. Identifying hazards that could cause potential harm
2. Evaluating risks of these hazards
3. Using systems engineering, find ways to lower the risk to levels, acceptable by society

Functional safety standards for the automotive industry in systems engineering - ISO 26262, is used to methodically reduce risk in passenger vehicle's electric/electronic systems.

Measures

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

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 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.]

Here are some characteristics of THIS Company's safety culture:

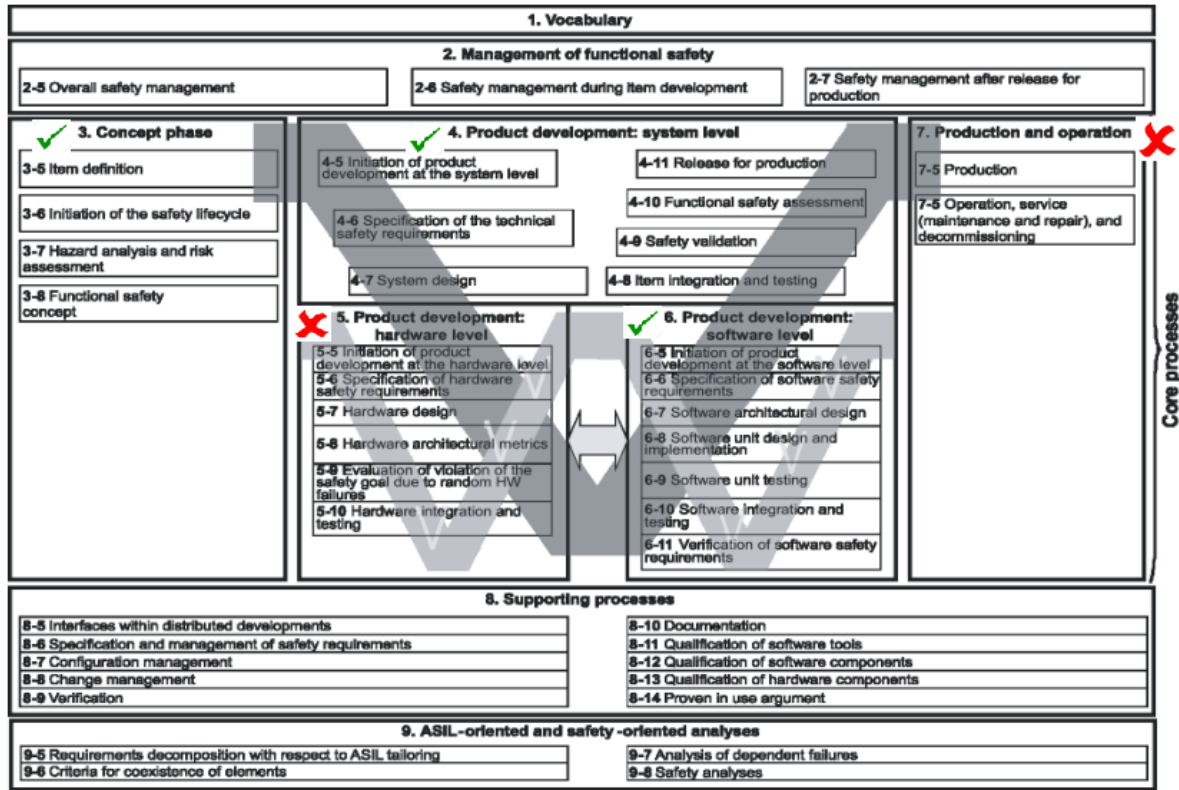
- **High priority:** safety has the highest priority among competing constraints like cost and productivity
- **Accountability:** processes ensure accountability such that design decisions are traceable back to the people and teams who made the decisions
- **Rewards:** the organization motivates and 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.]

This release cycle affects modification of an existing product. Hence, only a few steps in the ISO-26262 standards are applicable.

Safety life-cycle is tailored to include applicable sections as shown below.



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.

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
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 provides requirements or preliminary design to THIS Company.
 - THIS company develops the sub-system based on requirements or preliminary design and hands-over the developed functionality to OEM after independent testing.
 - OEM integrates the developed sub-system with the overall system and tests the functionality for completeness.

Confirmation Measures

Instructions: Please answer the following questions:

1. What is the main purpose of confirmation measures?

Confirmation measures ensure that the people who design the product and the people who review the design are independent.

Confirmation measures serve two purposes:

- A functional safety project conforms to ISO 26262, and
- The project really does make the vehicle safer.

2. What is a confirmation review?

Confirmation review ensure 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.