Safety Plan Lane Assistance

Document Version: [Version]

Template Version 1.0, Released on 2017-06-21

Document history

Date	Version	Editor	Description
01/23/18	1	Vijayakumar K	Initial Version

Table of Contents

Introduction

Purpose of the Safety Plan

A safety plan provides an overall framework for a functional safety project.
The safety plan defines the

- Item Definition
- Goals and Measures
- Safety culture
- Safety Lifecycle Tailoring
- Safety Management Roles and Responsibilities
- Development Interface Agreements
- Confirmation Measures

Scope of the Project

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

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

Lane Assistance System: This system will vibrate the steering wheel if it detects a lane departure and will move the steering wheel so that the wheels turn towards the center of the lane.

Two Main Functions are:

- 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

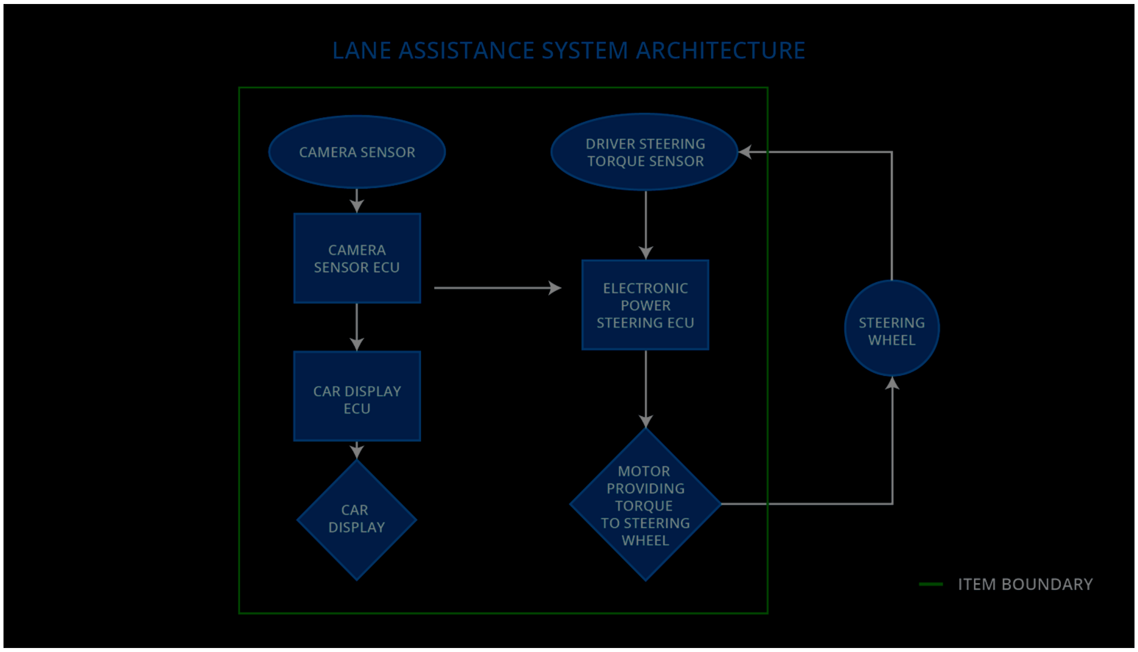
When the driver drifts towards the edge of the lane, two things will happen:

- 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.

Sub-systems are responsible for each functions are:

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

Item boundary is given below which shows the three sub-systems:


LANE ASSISTANCE SYSTEM ARCHITECTURE
CAMERA SENSOR
CAMERA SENSOR ECU
CAR DISPLAY ECU
CAR DISPLAY
DRIVER STEERING TORQUE SENSOR
ELECTRONIC POWER STEERING ECU
MOTOR PROVIDING TORQUE TO STEERING WHEEL
STEERING WHEEL
ITEM BOUNDARY

Goals and Measures

Goals

The main goal in functional safety is to reduce risk to acceptable levels. 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

Measures and Activities	Responsibility	Timeline
Follow safety processes	All Team Members	Constantly
Create and sustain a safety culture	Project 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 Manager	3 months prior to main assessment
Perform functional safety assessment	Safety Assessor	Conclusion of functional safety activities

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

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

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

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

1. 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. Responsibilities

Responsibilities for OEM

Functional Safety Manager- Item Level

- 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

Functional Safety Engineer- Item Level

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

Project Manager - Item Level

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

Responsibilities for my company

Functional Safety Manager- Component Level

Functional Safety Engineer- Component Level

Confirmation Measures

1. Main purpose of confirmation measures
   Confirmation measures serve two purposes:

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

The people who carry out confirmation measures need to be independent from the people who actually developed the project.

2. 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.

3. 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.